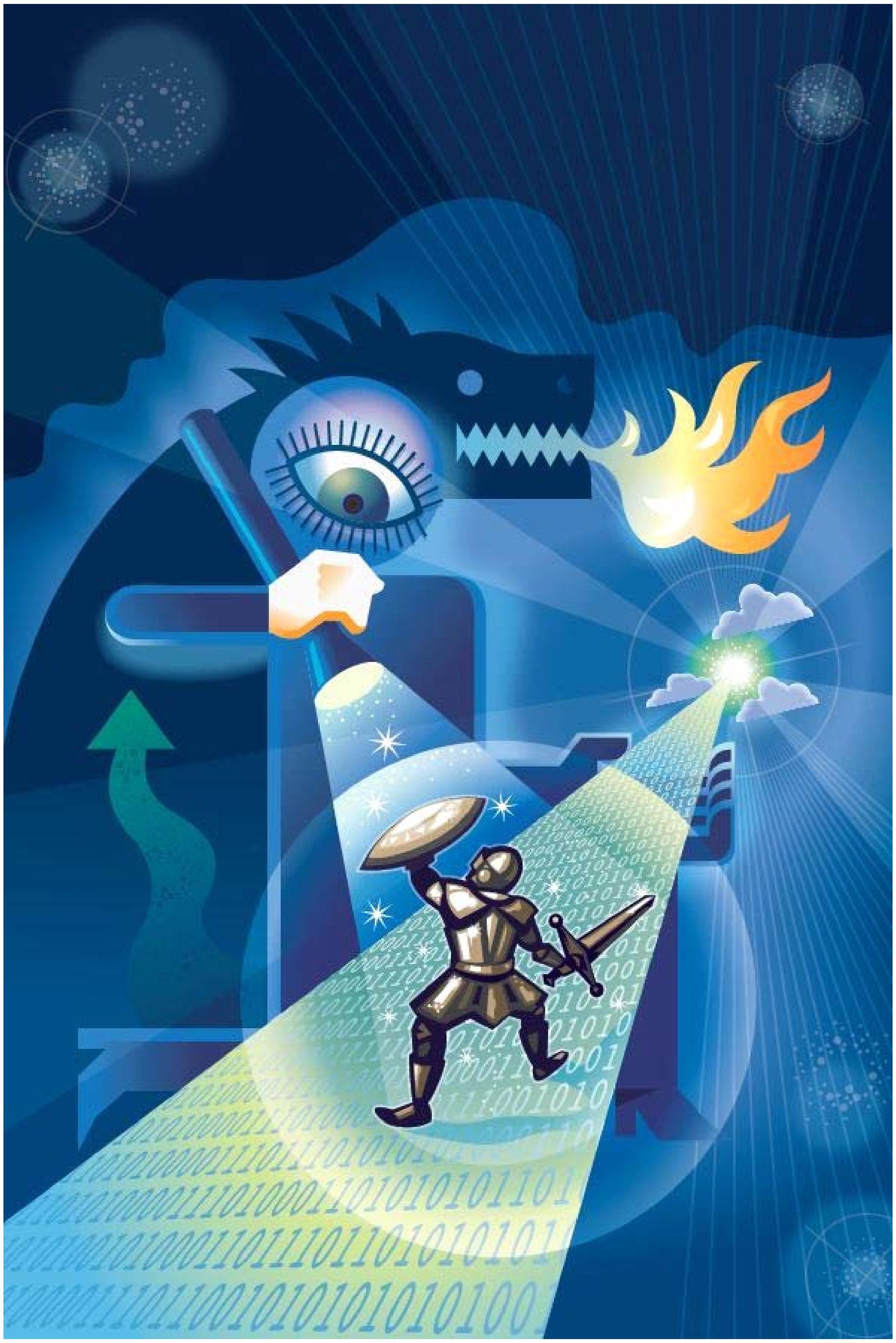
Cisco PCI Solution for Retail 2.0 Design and Implementation Guide

Last Updated: October 14, 2011



Cisco Validated Design

Solution Authors

Christian Janoff

Bart McGlothin

Christian Janoff, Vertical Solutions Architect, CMO ISE, Cisco Systems

Christian Janoff is a Retail Architect at Cisco Systems. with over 15 years of industry experience. Christian leads Cisco's participation on the Payment Card Industry Security Standards Council. He was elected to the PCI Council's Board of Advisors in May, 2009. Prior to Cisco, Christian worked as a network engineering manager at Safeway, Inc. Christian holds a bachelors degree from University of California at Santa Cruz

Bart McGlothin, Vertical Solutions Architect, CMO ISE, Cisco Systems

Bart is a Retail Architect at Cisco Systems. With over 15 years of industry experience, Bart leads Cisco's involvement with the National Retail Federation's Association for Retail Technology Standards Committee. Prior to Cisco, Bart worked as the Network Architect at Safeway, Inc.

Partner Authors

Rob McIndoe	Aaron Reynolds

Contributors

Mike Adler	Tom Hua
Mark Allen	Raymond Jett
Annette Blum	Manny Kamer
Renata Budko	Rekha Krishna
John Carney	Paul Lysander
Danny Dhillon	Fernando Macias
Michael Dugan	Bob Nusbaum
Zeeshan Farees	Manu Parbhakar
Carol Ferrara-Zarb	Vikram Prabhakar
Syed Ghayer	Jim Rintoul
Sujit Ghosh	Brian Robertson
Manisha Gupta	Angel Shimelish
Jamey Heary	Rick Simon
Gary Halleen	Maria Sisiruca
Stuart Higgins	Sheri Spence
Amanda Holdan	Greg Varga

CONTENTS

CHAPTER 1

Solution Overview

The Payment Card Industry Data Security Standard (PCI DSS) is generally perceived to be a complicated means to secure sensitive information. As of 2010, according to the PCI Security Standards Council, 100 percent of all breached companies were not compliant at the time of the breach, regardless of whether they were compliant at the time of their audit. How did a company that took such pains to achieve compliance not take equal measures to maintain it? Is the standard really so complex that it is not capable of being sustained? Some pundits have argued that PCI is therefore an unrealistic goal and valueless.

Cisco takes a more balanced stance. PCI is not overly stringent from a security perspective. In fact, Cisco sees the PCI security standard to be the *minimum* security any company should have when taking payments. PCI is a global attempt at setting a minimum bar. Some very large companies and some entire countries have not developed a security awareness that meets the evolved threats of cybersecurity today. From that perspective, PCI is the lowest common denominator that provides the minimum level of protection. Putting in a firewall, changing default passwords, locking the door to the wiring closet, and making sure that you have knowledge of who is configuring a device rather than leaving open a general admin account; these items are not complex.

Although the standard is indeed intricate, the real complexity challenge comes from managing an enterprise network. Enterprise companies do not arise overnight. Most companies that existed in the 1980s did not consider data security to be an ingredient that must be included at all levels. After IP became the de facto network protocol, enterprise companies have been struggling to integrate data with voice systems, video, wireless, digital media, administrative duties, and business processes; as well as holistically integrate protection of payment card information throughout. Each of these technologies was developed independently of each other. With the advent of IP, they have merged, in sometimes inefficient and complex fashion.

Therefore, the real struggle is to develop a simple, sustainable, and operationally efficient enterprise architecture. This foundation needs to have security integrated not only within its technical infrastructure but within its processes and policies as well. This manual is written to provide resources to address these issues and to help simplify compliance.

Executive Summary

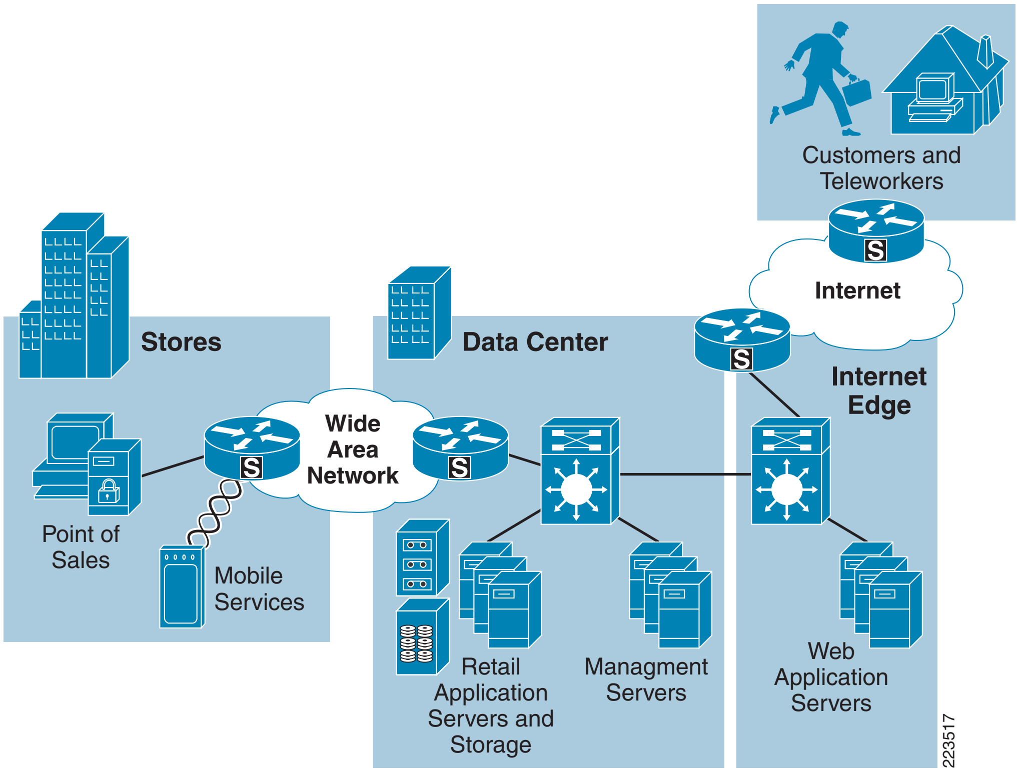
The Cisco PCI Solution for Retail 2.0 was developed to help retailers simplify and maintain PCI compliance. The solution consists of strategic guidance as well as tactical implementation. Cisco is in the unique position to apply its enterprise-wide architecture experience to the requirements of PCI. The Architectural Design section discusses what retailers should consider when designing their posture for addressing PCI. It examines enterprise architecture and discusses the related controls within them. The Implementation section provides specific design examples of these architectures, addressing PCI requirements using Cisco and Partner technology. Next, this document separates those architectures into their components. Each component is individually assessed for its capabilities, and configuration examples are given to demonstrate this utility. The solution shows how each component was assessed by Verizon Business and gives implementation examples and design considerations. Finally, the Reference Architecture Report by Verizon Business is appended at the end. The solution is designed to conform to PCI DSS 2.0.

The solution was built and tested using a holistic enterprise perspective including the following:

- Application consideration—Point-of-sale (POS) systems and payment devices, including wireless payment devices
- Administrative concerns within scope of PCI
- Cisco, RSA, EMC, VCE, and HyTrust network infrastructure
- Assessment by a qualified security assessor (Verizon Business)

The result is a set of retail store, data center, and Internet edge architectures and designs that simplify the process of a retailer becoming PCI compliant, maintaining that posture and providing the capability of awareness when under attack. (See Figure 1-1.)

Figure 1-1 Enterprise Architecture



Target Market/Audience

This solution is targeted toward the following audiences:

- Technical or compliance-focused individuals seeking guidance on how to holistically design and configure for PCI compliance
- Retailers that require a qualified security assessor to provide a Report of Compliance
- Retailers interested in preparing for growth that will someday require a Report of Compliance.

Although all retailers that take credit cards are required to be PCI compliant, this solution is designed to help the larger companies simplify the complexity of compliance. Smaller companies can benefit from the design and guidance as well, but should consult their acquiring banks for specifics if they do not currently require an onsite audit. Specific card programs are available at the following locations to determine their specific categorization process;

- American Express—http://www.americanexpress.com/datasecurity
- Discover Financial Services—http://www.discovernetwork.com/fraudsecurity/disc.html
- JCB International—http://www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide—http://www.mastercard.com/sdp
- Visa, Inc.—http://www.visa.com/Cisp

Solution Benefits

This solution demonstrates how to design end-to-end enterprise systems that conform to PCI DSS 2.0 guidelines. Companies can simplify the process of becoming PCI compliant by building a similar network with the recommended configurations and best practices. In addition, this solution provides the following benefits:

- Insight into the Cisco Connected Retail enterprise architecture and the controls used to address PCI
- A detailed analysis and mapping of Cisco and Partner components and their relationship with PCI DSS sub-requirements
- A scalable set of architectural designs that can be used as a reference during the PCI compliance process
- Insight into compensating controls and best practices to harden retail network and data systems
- A centralized management tool kit, which provides operational efficiency compared to managing the distributed endpoints individually
- Insight into the PCI audit process by providing a lab model and associated reference architecture report from Verizon Business

PCI Solution Results

Table 1-1 provides a summary of the PCI assessment results.

Table 1-1 PCI Assessment Results Summary

Component	Primary PCI Function		Component	Primary PCI Function
Endpoints and Applications			**Infrastructure**	
Cisco Unified CM and IP Phones	9.1.2		Cisco store routers	1.3, 11.4
Cisco Video Surveillance	9.1.1		Cisco data center routers	1.2, 1.3
Cisco Physical Access Control	9.1		Cisco store switches	9.1.2, 11.1b, 11.1d Segmentation
Cisco IronPort Email Security Solutions	DLP		Cisco data center switches	1.2, 1.3, 11.4
Cisco UCS	Servers		Cisco Nexus 1000V Series Switch	Segmentation
Cisco UCS Express on Cisco SRE	Servers		Cisco Nexus data center switches	Segmentation
Scope Administration			Cisco Wireless	4.1, 11.1
Cisco ACS	7.1		Cisco MDS Switch	3.4
RSA Authentication Manager	8.3		Cisco ASA-store	1.3, 11.4
HyTrust Appliance	10.5		Cisco ASA-data center	1.3, 11.4
Cisco Security Manager	1.2		Cisco FWSM-data center	1.3
EMC Ionix NCM	1.2.2		Cisco Nexus VSG	Virtual firewall
RSA Data Protection Manager	3.5		Cisco IDSM-data center	11.4
EMC CLARiioN	Storage		Cisco TrustSec	7.1, 11.1b, 11.1d
RSA enVision	10.5			

CHAPTER 2

PCI and the Solution Framework

The PCI Data Security Standard (PCI DSS) provides guidance for securing payment card data. It includes a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS provides an actionable framework for developing a robust payment card data security process, including prevention, detection, and appropriate reaction to security incidents. The current version is PCI DSS 2.0.

Table 2-1 lists the PCI DSS goals and requirements.

Table 2-1 PCI Data Security Standard (PCI DSS)

Goals	PCI DSS Requirements
Build and maintain a secure network	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	**5.** Use and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement strong access control measures	**7.** Restrict access to cardholder data by business need-to-know **8.** Assign a unique ID to each person with computer access **9.** Restrict physical access to cardholder data
Regularly monitor and test networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an information security policy	**12.** Maintain a policy that addresses information security for all personnel

The PCI DSS standard uses these 12 tenets to define how companies should secure their systems, both technical and social.

PCI DSS 2.0—New Reporting Guidelines

With PCI DSS 2.0, more thorough evidence is required from the merchant. This fact will not likely be called out anywhere within the PCI DSS 2.0 "Summary of Changes" document.

Historically, the PCI Security Standards Council (SSC) has provided qualified security assessors (QSAs) with a PCI "Scoring Matrix" document, which has provided the validation and reporting requirements for each PCI DSS requirement. For example, one requirement may require the QSA to review a supporting document and process to confirm a requirement is in place, where another may require that a document (for example, a policy or procedure document) as well as configuration and/or system settings be examined.

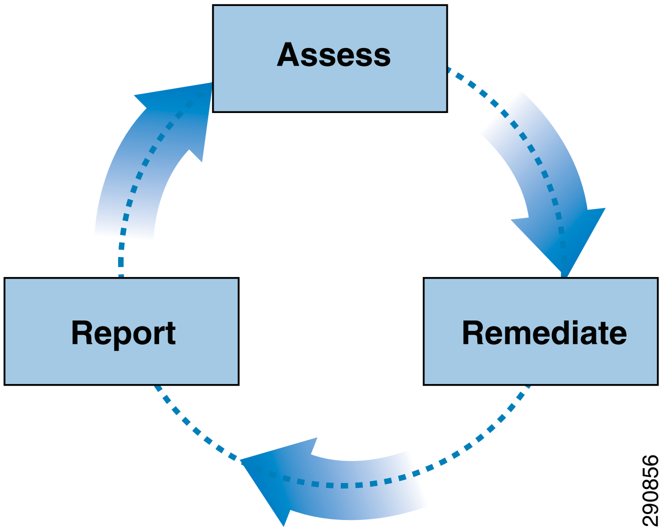
The Scoring Matrix has been replaced by a "Reporting Instructions" document. The necessary validation steps have been expanded. There is a greater level of detail required for assessor documentation (for example, observation of documentation, observation of process, action, or state, observation of configuration file/system settings, observation by interview, and so on).

These new instructions will likely lead to a more thoroughly conducted assessment.

Maintaining PCI Compliance

As stated in the overview, becoming compliant is not the real challenge associated with PCI. Although many companies view becoming compliant as a goal or an endpoint, it is better to view PCI as a continuous cycle rather than a snapshot in time (see Figure 2-1). This may seem intuitive, but many organizations relax after passing an audit. Rather than preparing for the ongoing activity of maintaining compliance, the posture that allowed the organization to pass degrades over time. Compliance is assumed to be continuous.

Figure 2-1 Continuous Compliance Cycle



A good model to adopt is one that looks at the full spectrum of time for maintaining and simplifying compliance:

- Future: Become compliant—What is the current state of the organization compared to the compliant state? What changes are needed to reach a state of compliance? Is there a new standard on the horizon or are there pending changes to the organization that might affect the state of compliance? Are there new store openings or mergers? What preparations are needed, both from a technical and process perspective, to account for maintaining compliance?
- Present: Know that you are still compliant—What tools are being used to recognize that the organization is in a state of compliance? Are there application dashboards that are succinctly developed to provide a current state of compliance? Is there a department or set of departments that "own" this state? Are there accurate diagrams and documentation for the full scope of the company that is within the scope of compliance?
- Past: What happened to the compliance?—Did someone in the organization turn rogue? Did someone from the outside break in? Did someone "fatfinger" a command? Who did? How can you account for what systems are in scope and gain forensic knowledge to account for who is doing what?

This solution is designed to provide the tools and design practices to help answer these questions.

Cardholder Data Environment and Scope

One of the most important concepts within PCI is the scope or the size of the merchant's cardholder data environment (CDE). This is important for several reasons: the CDE comprises the specific applications, systems, and associated personnel that have access to sensitive data. This is the range of infrastructure and people that must successfully pass an audit to become PCI compliant. More importantly, this is also the area that must be properly maintained to be safe from the threat of a hacker. The term *sensitive data* refers to the items listed in Table 2-2, provided by the PCI DSS standard.

Table 2-2 Guidelines for Cardholder Data Elements

		Data Element	**Storage Permitted**	**Render Stored Account Data Unreadable per Requirement 3.4**
Account Data	**Cardholder Data**	Primary account number (PAN)	Yes	Yes
		Cardholder name	Yes	No
		Service code	Yes	No
		Expiration date	Yes	No
	Sensitive Authentication Data	Full magnetic stripe data	No	Cannot store per Requirement 3.2
		CAV2/CVC2/ CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN block	No	Cannot store per Requirement 3.2

Wherever the data that corresponds to the fields in Table 2-2 are present in your organization, the appropriate measures must be taken to secure them.

PCI Best Practices

“Limit scope, protect it, maintain it…”

When it comes to simplifying PCI, this is probably the best advice:

> “Limit the size of the scope of your cardholder data environment, protect the area within the perimeter of that environment, and then strive to maintain it as efficiently as possible.”

This guide demonstrates on many levels how pervasive this philosophy should be taken. *Limiting the scope* really means challenging your company. Challenge your management. Challenge the business. Challenge your department to weigh the risk versus the benefit of its current way of doing business. This does not necessarily mean that you must change. However, looking skeptically at the actual needs of the business combined with the sobering reality that there are organized criminals striving to steal from your company, you can systematically identify and document the true scope of your PCI environment and refine it to its core requirements. Minimizing the overall PCI scope and reducing unnecessary systems or unjustified access to systems reduces the ongoing requirements of PCI and simplifies the overall compliance cost and maintenance.

Several factors must be considered to maximize the efficacy of this philosophy. You must accurately determine the existing scope of what you have to secure before you can look at how to refine it. The following sections of this chapter discuss considerations of what might be in scope for your organization, and consequently your deployment using the Cisco solution framework for compliance.

The second part of the advice is to protect the area within the perimeter of the retailer’s scope. The majority of this manual gives guidance at varying levels of detail on how and where to implement controls for secure payment processing. Guidance is given from the architectural, design, and component perspectives to provide a comprehensive solution for protecting the cardholder data environment.

The final piece of the advice is to maintain it as efficiently as possible. The best way for retailers to ensure that this important aspect is not overlooked is to adjust their organizations to include a role within the organization that owns this responsibility. Many times, boards or representatives of different parts of the organization are brought together to develop a state of compliance. Without a clear owner of ultimate responsibility, retailers can sometime suffer from diffusion of responsibility, and compliance can be lost within the cracks of silos of large organization. By defining a person or group that identifies this as a chartered responsibility, retailers can ensure a focal point of identifying new risks as the retailer changes over time.

Scope Maintenance

Documenting all known applications, their services, and systemic requirements from source to destination is required to fully understand the true range of the scope. This also provides a baseline to compare against for the ongoing requirement to ensure that scope does not unknowingly increase. This is also the area to apply that dose of skepticism. As the applications that are involved with payment card information are catalogued, determine whether any of the functionality can be maintained while removing sensitive data.

New PCI DSS 2.0 language has been added to clarify the merchant’s responsibility to discover and validate the PCI DSS scope within their environment, through a formally documented methodology.

From the PCI DSS 2.0 standard (page 10 under "Scope of Assessment for Compliance with PCI DSS Requirements"):

> *The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope. To confirm the accuracy and appropriateness of PCI DSS scope, perform the following:*
>
> - *The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined cardholder data environment (CDE).*
> - *Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).*
> - *The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE unless such data is deleted or migrated/consolidated into the currently defined CDE.*
> - *The entity retains documentation that shows how PCI DSS scope was confirmed and the results, for assessor review and/or for reference during the next annual PCI SCC scope confirmation activity.*

Changes to personnel, additions of new systems, addition of new stores, removal of obsolete accounts or systems, and anything else that affects the state of compliance should be exposed as a factor in a retailer's compliance maintenance program. Monitoring which applications are accessing sensitive data and through which infrastructure systems must be updated on a regular basis. The PCI standard does not specify a method, so merchants can determine the best methods for their specific situations.

One option to comprehensively discover sensitive cardholder data is through the RSA Data Loss Prevention (DLP) Suite, which can accurately identify the location and flow of cardholder data throughout an environment. After files with sensitive information are identified and classified, they can be copied, moved, archived, deleted, or secured based on policy. The RSA DLP Suite is available in three modules:

- RSA DLP Datacenter can identify cardholder data and enforce policies across file shares, databases, storage systems (SAN/NAS), Microsoft SharePoint sites, and other data repositories.
- RSA DLP Network can identify cardholder data and enforce policies across corporate e-mail systems, web-based e-mail systems, instant messaging, and web-based protocols.
- RSA DLP Endpoint can identify cardholder data and enforce policies for such data stored or in use on laptops and desktops.

Each DLP module is centrally managed by the RSA DLP Enterprise Manager, a single browser-based management console. The RSA DLP Enterprise Manager offers dashboard, incident workflow, reporting, policy administration, and systems administration functionality.

Freeware applications such as the following can also be used to help document where your sensitive data resides:

- Spider
- SENF
- Snort
- Nessus

Cardholder Data Environment—Scope Layers

The following sections describe the three layers of the cardholder data environment.

Endpoints and Applications

Any endpoint or application that passes sensitive data needs to considered and secured from an end-to-end perspective. The following sections provide examples.

Point-of-Sale

Point-of-sale applications in the store are the obvious candidates for documenting. Others include applications that access and use this sensitive information for other business processes. For example, customer relation management (CRM) applications are sometimes commingled with their customer's credit card data for customer data mining.

E-commerce and Public-facing Websites

Web applications continue to be a major point of entry for hackers. "SQL injections" are one method that hackers use to exploit poorly written front-end applications. E-commerce applications obviously need to be tested for vulnerabilities. However, *any* front-end web application should be treated with equal scrutiny. Some large breaches have occurred when a hacker was able to compromise a Human Resources website that accepted resumes. Defense in depth is needed across all perimeters, and any front-end application needs to have minimum standards.

Voice

Voice systems are not specifically called out in the standard. However, the standard is clear that entities must secure all systems that transmit cardholder data. Therefore, your entire voice system may be in scope depending on how sensitive data is being used. Are you taking phone payments? Are you recording sensitive data in a contact center? Are you using applications that take cardholder data over interactive voice response systems? Cisco phones have built-in Ethernet interfaces that can be used to connect to downstream registers. This saves wiring costs but puts the phone into scope, because it is now a system transmitting cardholder data.

Physical

Video surveillance systems that monitor the sensitive areas such as wiring closets within stores are considered to be part of the scope of compliance because they can document who had access to a sensitive physical area. Administrators of these systems are also considered to be in scope.

E-mail

Cisco does not recommend taking credit card payment information using e-mail. However, if this does occur, e-mail systems and clients would all be in scope.

Scope Administration

Any piece of hardware that transmits sensitive data is considered to be in scope. Therefore, administration of those devices brings those administrative applications and administrators into scope.

People

Administrators who have access to the systems that process, transmit, or store sensitive data are also in scope. Strive to limit access to "business need-to-know" personnel. Clear role definitions can greatly reduce the population that can compromise your company by removing access for people that really do not require access to do their jobs. Approximately one-third of the breaches that occurred in 2009 were from internal personnel (2010 Verizon IBR). Restrict the administrative rights of your personnel to access systems that have sensitive data by allowing administrators privileges based only on the "need-to-know". This can dramatically reduce the risk to your company and in event of a breach, reduce the range of candidates for a post-breach audit.

Processes

PCI compliance is typically not the only standard that must be addressed. Design your security policy to be as streamlined and efficient as possible while maintaining flexibility for other compliance regulations. Examples of common overlapping compliance standards include Sarbanes Oxley or the Health Insurance Portability and Accountability Act (HIPAA). When developing an efficient holistic security policy, processes must be designed to minimize overall complexity for issues such as change control and administrative access and procedures.

Storage of Sensitive Information

Wherever sensitive information is stored, it must be encrypted. Storage area networks and in-store processors are the main areas where encryption and key management procedures are applied. Virtual environments and cloud services should be heavily scrutinized for simplistic methods of compliance procedures.

Monitoring

Tools that provide the following monitoring capabilities are in scope:

- Real-time anomalous behavior
- Historical forensic analysis
- Configuration analysis to enforce template standards

Infrastructure

The physical infrastructure involved with the card data environment needs to be considered from an end-to-end perspective. Traditional components include firewalls, switches, routers, wireless access points, network appliances, and other security devices. Virtualization components such as virtual switches/routers, virtual appliances, and hypervisors that store, process, or transmit cardholder data are also in scope. Not all of the systems are obvious. Sometimes devices such as load balancers, WAN application acceleration devices, or content engines are overlooked and can be a source of compromise because these devices were not considered.

Architectural Sampling

One of the methods for reducing complexity is to standardize on architectures. For example, if you are able to replicate a standardized build across systems within the store, auditors can take a sample of the total population of stores rather than having to audit every single store. However, a common misperception is that only the stores that are audited are in scope. All branches are assumed to follow exactly the same build and procedures to use a sampling method. Be clear that in the event of a breach, a post audit will determine whether proper controls were applied across *all* branches. If this is found not to be the case, the merchant may be liable for litigation.

Partners

Any business partner that connects to your network with access to sensitive data needs to be PCI compliant. There must be a signed agreement for culpability that designates responsibility and demarcation between the two companies.

Service Providers

Any service provider that connects to your network with access to sensitive data needs to be PCI compliant. There must be a signed agreement for culpability that designates responsibility and demarcation between the two companies.

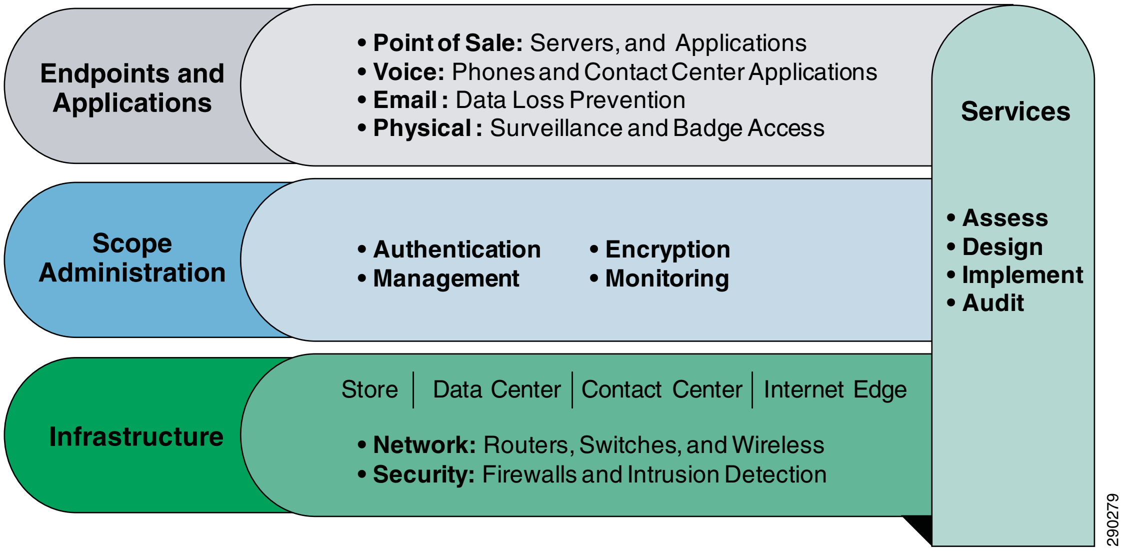
Internet

The Internet is a large public network that introduces a host of threats. Wherever direct Internet access is available, it should be considered a perimeter requiring a firewall and IDS/IPS technology to secure that access.

PCI Solution Framework

Figure 2-2 shows a comprehensive view of the elements previously discussed, and shows how the Cisco PCI Solution For Retail 2.0 organizes them into a solution framework.By using this framework, PCI can be simplified into three overarching layers that provide a simple way to discuss the complexity of the topic.

Figure 2-2 Cisco PCI Solution for Retail 2.0 Solution Framework


Endpoints and Applications
• Point of Sale: Servers, and Applications
• Voice: Phones and Contact Center Applications
• Email : Data Loss Prevention
• Physical : Surveillance and Badge Access
Scope Administration
• Authentication
• Management
• Encryption
• Monitoring
Infrastructure
Store
Data Center
Contact Center
Internet Edge
• Network: Routers, Switches, and Wireless
• Security: Firewalls and Intrusion Detection
Services
• Assess
• Design
• Implement
• Audit
290279

The Cisco PCI Solution for Retail 2.0 framework is used throughout this guide as a model.

Endpoints and Applications

This layer of the solution takes into account any application or endpoint that is involved in the scope of a PCI audit. An application is defined as any that uses cardholder data *or* is not segmented away from the cardholder data environment (CDE). Examples of an endpoint include a point-of-sale (POS) server, POS register, surveillance camera, wireless line buster, and so on.

Scope Administration

This layer of the solution addresses areas of PCI compliance that affect the CDE at an administrative layer. It is defined by how systems are accessed (management and authentication), where sensitive data resides or is stored (encryption), and how alerts to this environment are used (monitoring).

Infrastructure

This layer of the solution framework addresses the infrastructure components such as routers, switches, firewalls, and security components.

Services

Services for designing, implementing, and auditing can be found from both Cisco and Verizon Business at the following URLs:

- Cisco—http://www.cisco.com/en/US/products/svcs/services_area_root.html
- Verizon—http://www.verizonbusiness.com/Products/security/

CHAPTER 3

Solution Architecture

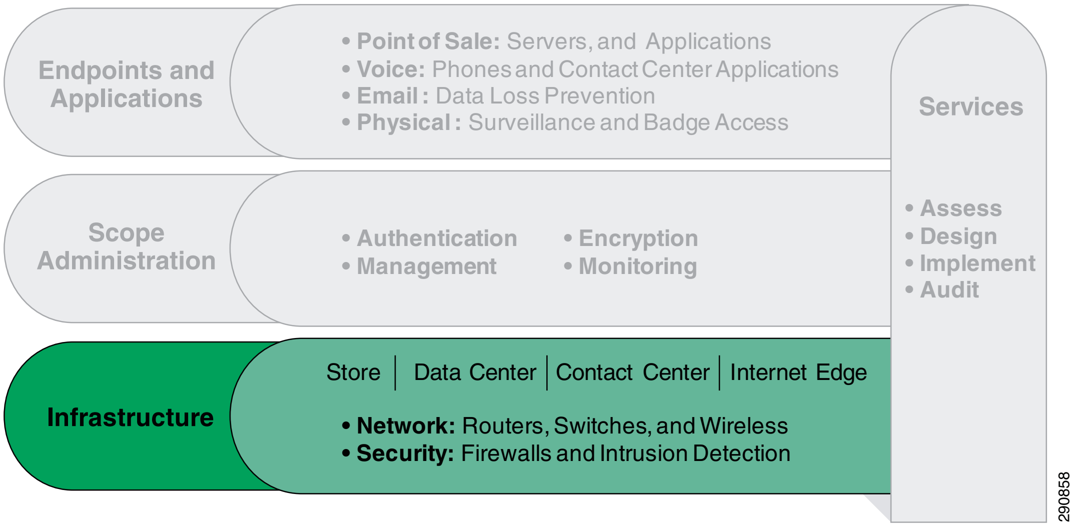
The Cisco PCI Solution for Retail 2.0 is a set of architectures, strategic principles, and tactical designs that details a holistic approach to addressing the requirements of PCI DSS 2.0. The Cisco Connected Retail architecture is used as a baseline for demonstrating the range of places that typically exist within an enterprise retailer. This chapter describes the Connected Retail Architecture in detail, so that when the discussion of specific PCI controls is discussed, the controls can be placed in context with that enterprise-wide view. The solution looks at an enterprise from an end-to-end perspective; from the store, where someone swipes the credit card, to the back-end of the data center, where the transaction leaves the retailers network to be processed by the acquiring bank. For more information on the Cisco Connected Retail Architecture, see http://www.cisco.com/go/retail.

For specific designs referencing these architectures, see Chapter 4, “Solution Implementation.”

For more information on the individual components used to build these architectures, see Chapter 5, “Component Assessment.”

Chapter 2, “PCI and the Solution Framework,” describes the elements that make up the solution framework. The solution framework organizes the scope of the cardholder data environment for contextual reference. The bottom layer of the model shows the organization of the enterprise into places such as the store, data center, and the Internet edge. (See Figure 3-1.)

Figure 3-1 Solution Framework

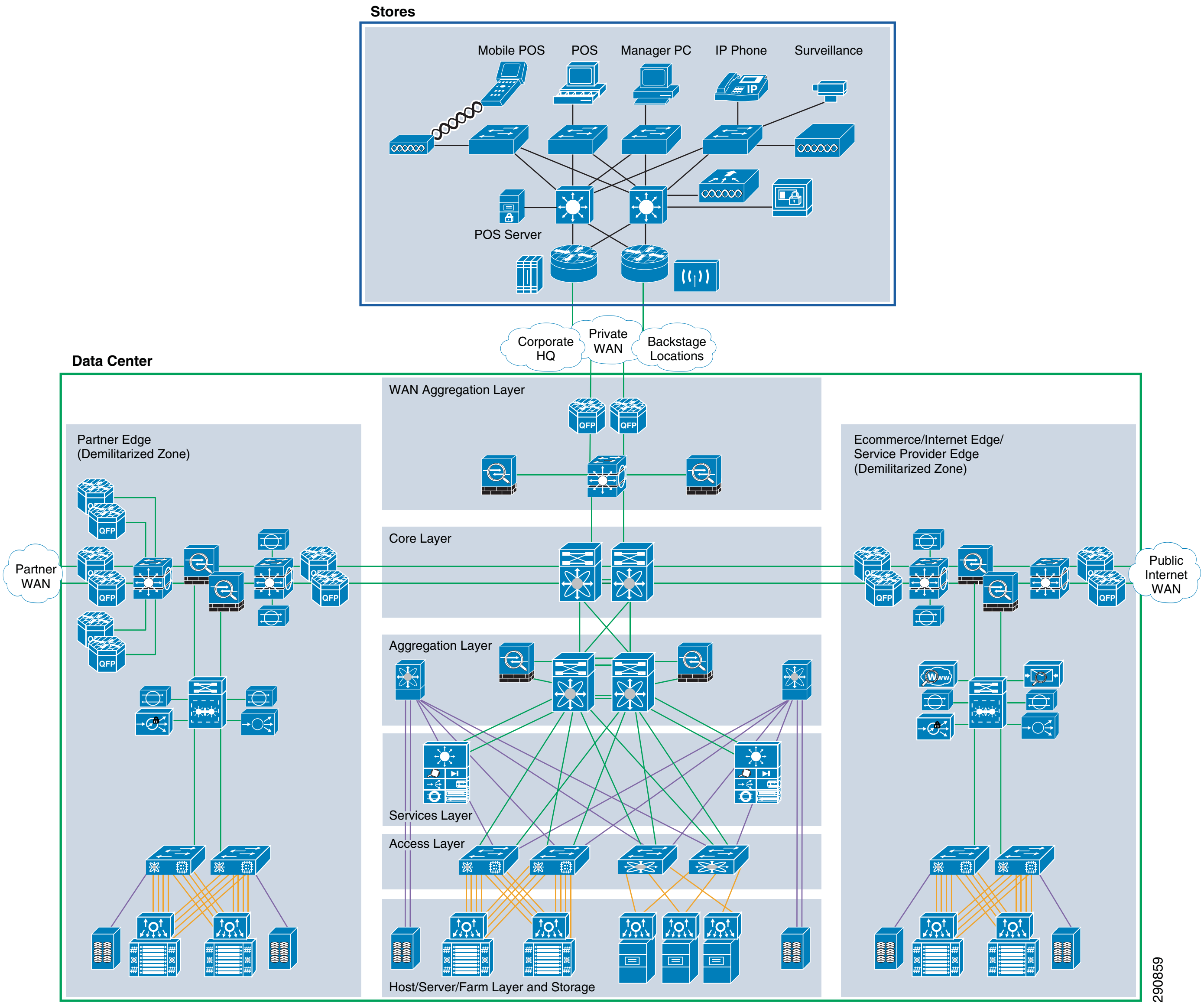

Endpoints and Applications
• Point of Sale: Servers, and Applications
• Voice: Phones and Contact Center Applications
• Email : Data Loss Prevention
• Physical : Surveillance and Badge Access
Services
Scope Administration
• Authentication
• Management
• Encryption
• Monitoring
• Assess
• Design
• Implement
• Audit
Infrastructure
Store
Data Center
Contact Center
Internet Edge
• Network: Routers, Switches, and Wireless
• Security: Firewalls and Intrusion Detection
290858

Enterprise Architecture and PCI Design Considerations

PCI compliance affects the overall enterprise architecture, depending on the requirements of the business. For example, a new business requirement for direct customer Internet connectivity at the store level extends the firewall and IDS/IPS perimeter requirements to the branch level, whereas before it might exist only at the headend data center. Without this contextual reference, it is difficult to discuss specific controls.

Figure 3-2 shows the enterprise-wide retail reference architecture and locations that commonly exist in the enterprise retailer domain.

Figure 3-2 Enterprise-wide Retail Reference Architecture



The following sections describe the major places affected by PCI compliance throughout the enterprise. Each section provides design considerations that are affected by PCI controls in more detail.

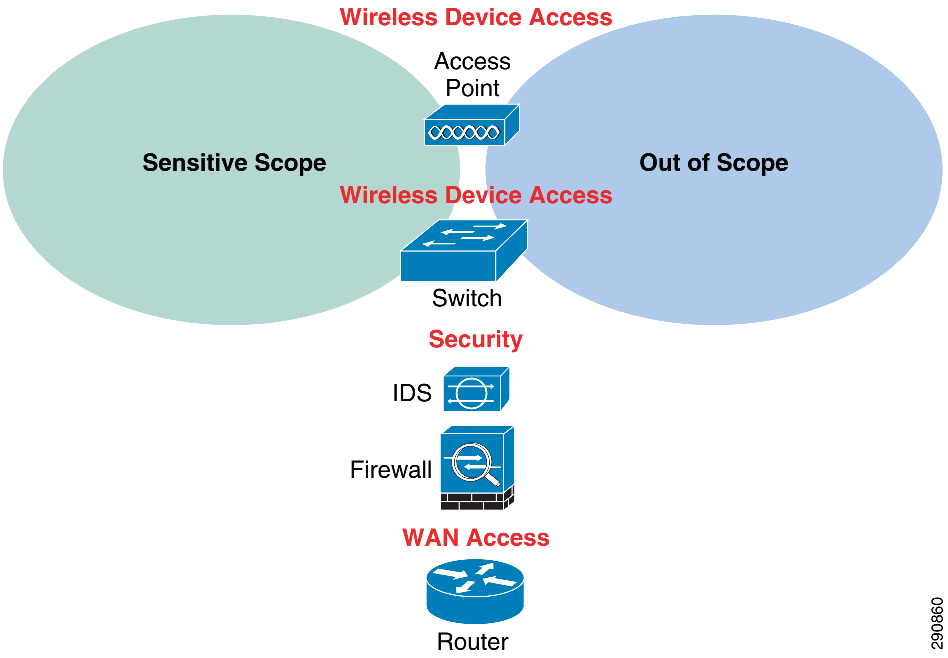
Store Architecture

The store is the location where customers swipe their credit cards to purchase goods. Depending on the type of services that are offered at the store, various levels of security are required. This section discusses those design considerations and relates them to various store formats.

Design Considerations

Figure 3-3 shows the fundamental infrastructure components used within a store location. These components are used in conjunction with each other to segment sensitive data from non-sensitive data. The process of segmenting the network into *scopes* allows a merchant to reduce the amount of branch-level components that need to be audited. Note that devices/endpoints themselves may be cut out of the scope of an audit by putting them onto their own network, but the actual network infrastructure may not necessarily be decreased. For example, a switch can have devices that are both sensitive and non-sensitive attached to it. By putting the non-sensitive devices onto their own VLANs, they can be cut out of the audit by using the VLAN function of the switch. However, the switch itself still remains in scope.

Figure 3-3 Fundamental Store Infrastructure Components



Each store component is used for a different function, as follows:

- The router function can be used for:
  - Accessing the WAN
  - Routing between VLANs
  - Access control lists
- The firewall can be used for:
  - Filtering unnecessary or inappropriate data via a stateful firewall
  - Routing between VLANs
  - Detecting and preventing intrusions; (IPS/IDS devices can also be separate appliances)
- Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS) monitor for anomalous behavior on the network and send alerts.
- The switch can be used for:
  - Segmenting via VLANs

  - Accessing wired devices
- The access point can be used for:
  - Wireless segmentation
  - Accessing wireless devices

The function of each of these devices can be virtualized and consolidated for simplicity, depending on the space and management requirements of the store footprint. For example, some smaller box stores have power, wiring closet, rack, and cabling restraints that would benefit from virtualized devices that reduce the physical footprint of the branch infrastructure.

Conversely, each of these devices can be increased in number depending on the resiliency and redundancy requirements of the business. For example, if store connectivity is a business priority, using redundant routers for redundant WAN access might be a requirement to ensure that store connectivity is maintained.

Regardless of how the store is designed from a redundancy or scale perspective, the same types/locations of controls are consistent across them.

Many retailers use their data center as their centralized location to connect to public networks such as the Internet. This perimeter is typically secured as a demilitarized zone (DMZ) using firewalls and IDS/IPS. Whenever you introduce any type of untrusted network (wireless, Internet, microwave, satellite, cellular, and so on) into the store environment, you have effectively created a new external perimeter that must now be secured with a firewall and intrusion detection/prevention system. Table 3-1 defines the types of factors that affect store controls and requirements.

Table 3-1 Store Services and Corresponding Compliance Controls Located at Store

Store Service Type	Minimum PCI Control Required	Relevant Solution Component
Any store with point-of-sale (POS) systems	Rogue detection	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x switch
POS systems; no direct Internet access, no wireless access, no untrusted networks of any type	Access control lists (ACLs), no state table required	Any router with ACLs
Basic wireless connectivity	Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS appliance
Wireless POS	Firewall, IDS, strong client encryption	Cisco ISR, Cisco ASA, Cisco IPS appliance, Cisco Unified Wireless
Public WAN	Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS appliance

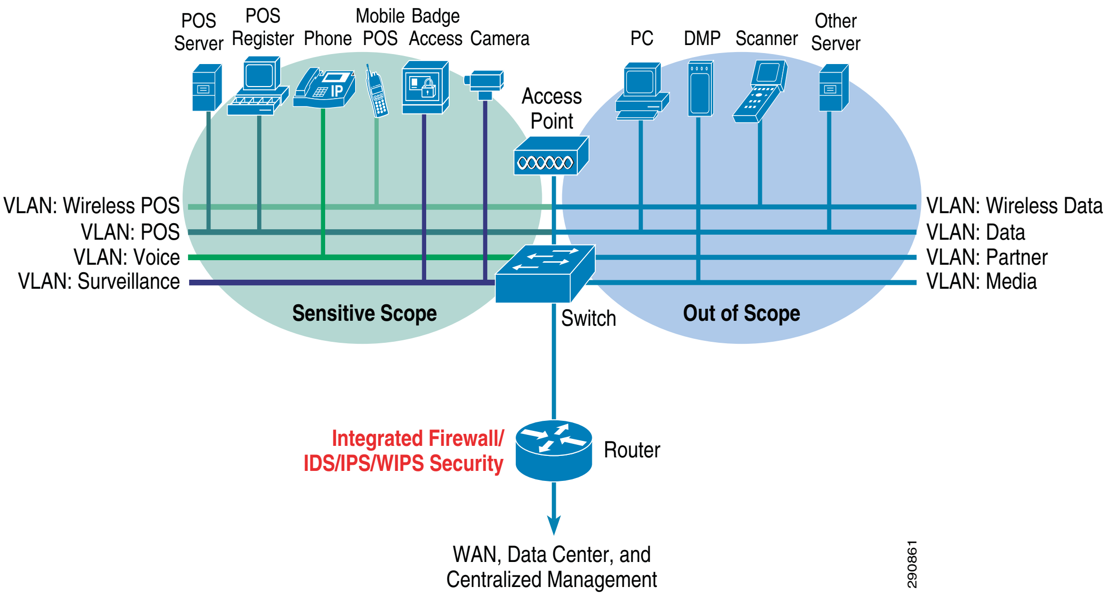
Table 3-1 Store Services and Corresponding Compliance Controls Located at Store (continued)

Internet connectivity	Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS appliance
Any untrusted network access	Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS appliance

The fundamental reference store architecture assumes that a retailer may eventually need to scale to these levels of services, but not necessarily immediately. From a store perspective, the Cisco Integrated Services Router (ISR) performs each of the functions listed in Table 3-1. This allows merchants to grow with their investment by purchasing a router that can scale by different license keys for different services without having to rip and replace. For example, a merchant can purchase a Cisco ISR for basic WAN connectivity. When the business wants to introduce wireless to the stores, the merchant can unlock the firewall/IPS/IDS feature set with a license.

The fundamental store reference architecture in Figure 3-4 shows the solution framework endpoints/applications within the context of the fundamental store component's infrastructure.

Figure 3-4 Fundamental Reference Store Architecture



In-scope devices can include the following:

- POS devices
- Wireless handheld devices
- Mobile POS
- Voice systems
- Physical badge access
- Video surveillance systems.

In general, an additional VLAN for management of infrastructure should be distinctly defined.

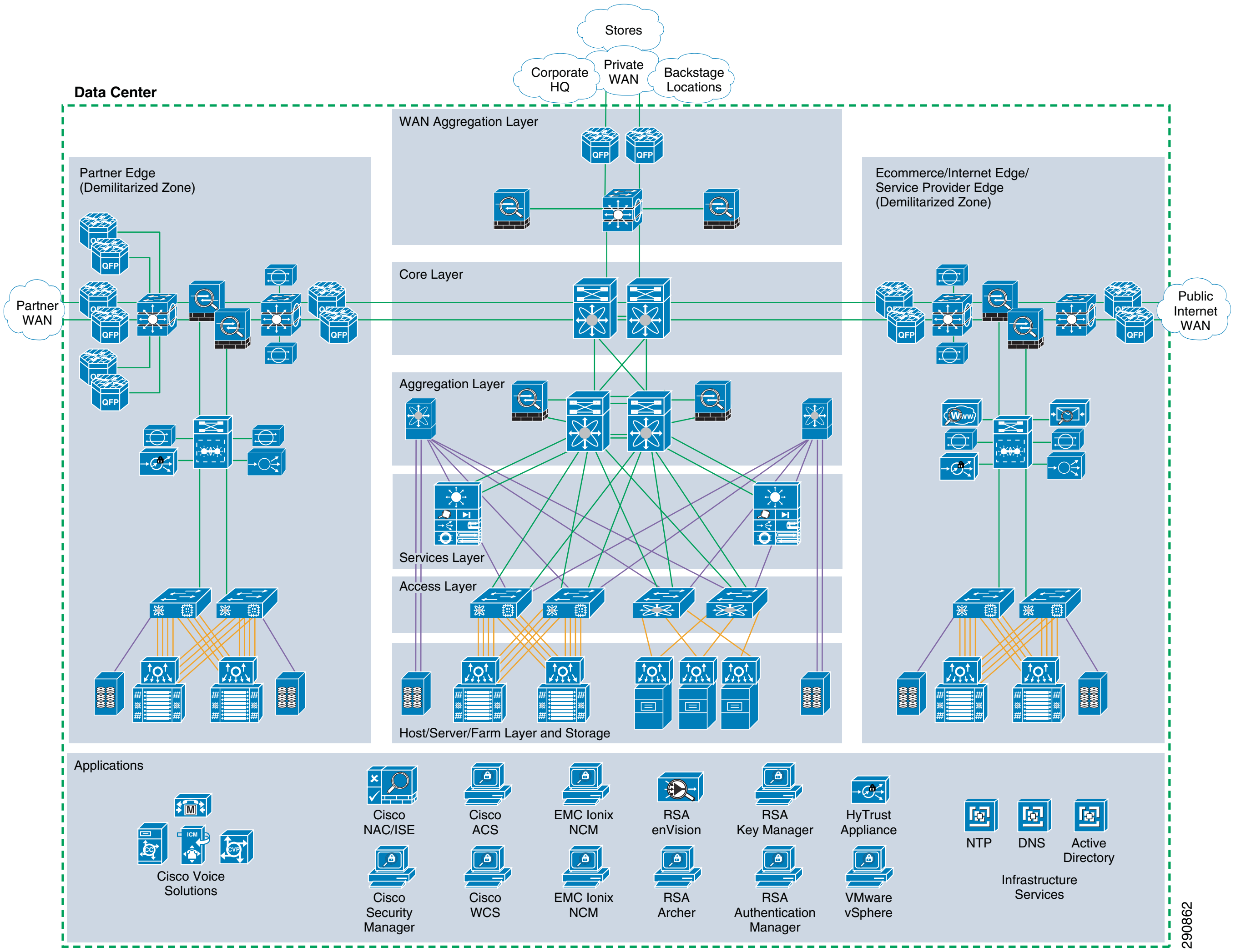
The remaining devices at the store level are considered *out-of-scope* and do not need to be audited, given that they are on their own network and segmented via firewall/IPS/IDS from the sensitive networks.

The PCI store model and its controls were applied to the small, medium, and large Connected Retail Store footprints and are shown in Chapter 4, "Solution Implementation," in detail. This section provides sample addressing plans used by various stores. Many designs can be extracted by understanding and using the PCI solution model shown above, but the overall functions are essentially the same.

Data Center

The data center is where centralized data processing, data storage, and data communications take place (see Figure 3-5). The data center is also the place where management systems are deployed. The data center provides centralized control from an administrative perspective because it is typically where the tools that are used to monitor and enforce compliance are deployed.

Figure 3-5 Data Center Architecture



Design Considerations

Design considerations are as follows:

- Centralized solution management that supports all aspects of network, security, and systems management; and supports remote access from anywhere on the network.
- Standardized equipment and software images, deployed in a modular, layered approach, that simplify configuration management and increase the availability of the system.
- A highly available data center design that permits highly resilient access from stores to core data and storage services.
- WAN aggregation alternatives that allow flexible selection of service provider network offerings.
- A service aggregation design that allows for a modular approach to adding new access layers and managing shared network services (for example, firewall, IDS, application networking, wireless management).
- Firewall, IDS, and application networking services that are available at the service and aggregation layers of the data center.
- Scalability that can accommodate shifting requirements in data center compute and storage requirements.
- Note that WAN access speeds are typically the limiting factor between the store network systems and the WAN aggregation layer. It is typical for retailers to over-subscribe the WAN circuits between the stores and the WAN edge aggregation router. Over-subscription can cause inconsistent results and packet loss of payment card information in the event that more traffic enters the WAN circuit simultaneously.
- Backup network connections from store networks to the data center are recommended when payment card information is transported via the WAN.

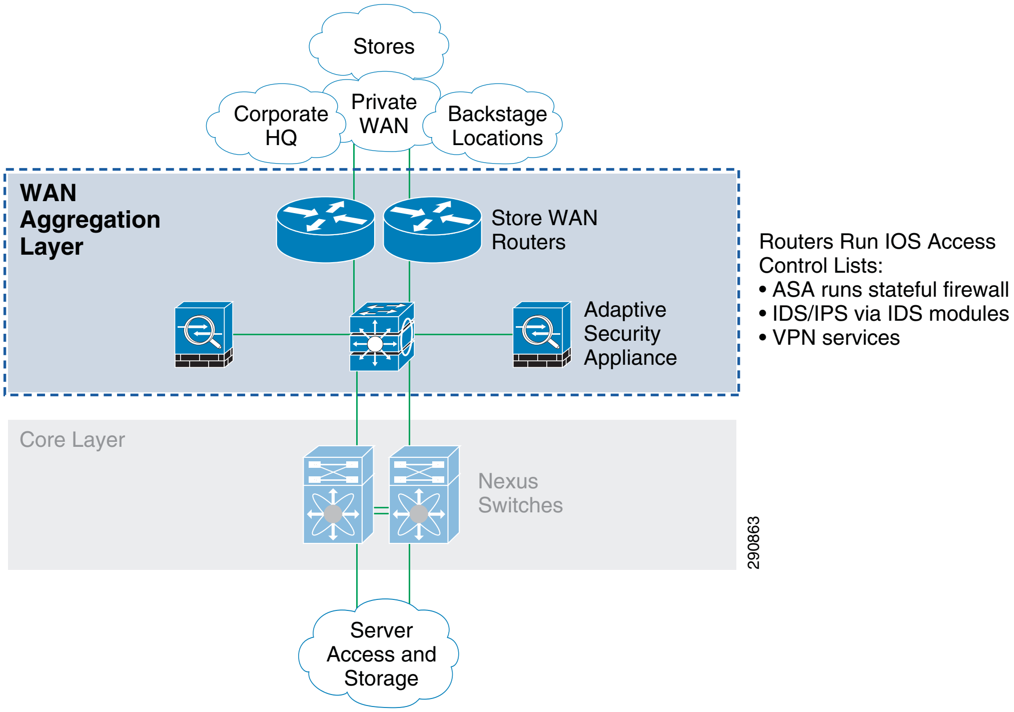
Data centers can house many types of functions, and the term itself can encompass narrow and broad aspects. For the purposes of this guide, data centers include the following functions:

- WAN aggregation layer—Aggregates the store and backstage WAN connections to the core
- Core layer—Highly available, high-speed area that is the central point of connectivity to all data center areas
- Aggregation layer—Aggregates the services of one area and connects that area to the core
- Services layer—Data treatment and manipulation occurs between the access layer and aggregation layer
- Access layer—Server-level access and connectivity between hosts/servers to the services and aggregation layers, depending on the nature of the application
- Host/server farm—Physical servers, virtualized servers, and appliances' host applications
- Storage—Storage area networks (SANs)
- E-commerce—Internet-based transactions
- Internet/service provider edge demilitarized zone (DMZ)—Secure connectivity to the Internet
- Partner edge DMZ—Secure segmented connectivity to partners

WAN Aggregation

The WAN aggregation layer is a transit network that aggregates the connections from the stores, backstage locations, and corporate offices, as shown in Figure 3-6.

Figure 3-6 WAN Aggregation Layer


Stores
Corporate HQ
Private WAN
Backstage Locations
WAN Aggregation Layer
Store WAN Routers
Adaptive Security Appliance
Routers Run IOS Access Control Lists:
• ASA runs stateful firewall
• IDS/IPS via IDS modules
• VPN services
Core Layer
Nexus Switches
290863
Server Access and Storage

Design Considerations

The WAN edge routers should not also be used as the Internet gateways for the data center network. By clearly defining zones of separation of responsibility within the infrastructure, it is easier to maintain.

Two options are possible at this layer for Layer 3 filters at the WAN aggregation layer:

- Firewall appliance—Interior to the WAN edge routers, a dedicated firewall appliance is used to secure incoming WAN traffic and to terminate store VPN connections. This design provides the highest scalability.
- Cisco IOS Software firewall routers—Many Cisco routers also support the Cisco IOS Security Software option that includes a firewall feature. Cisco recommends the use of the Cisco IOS Security feature set in stores, branches, and teleworker deployments, because of a much lower number of users and connection rates than at the store WAN aggregation headend location.

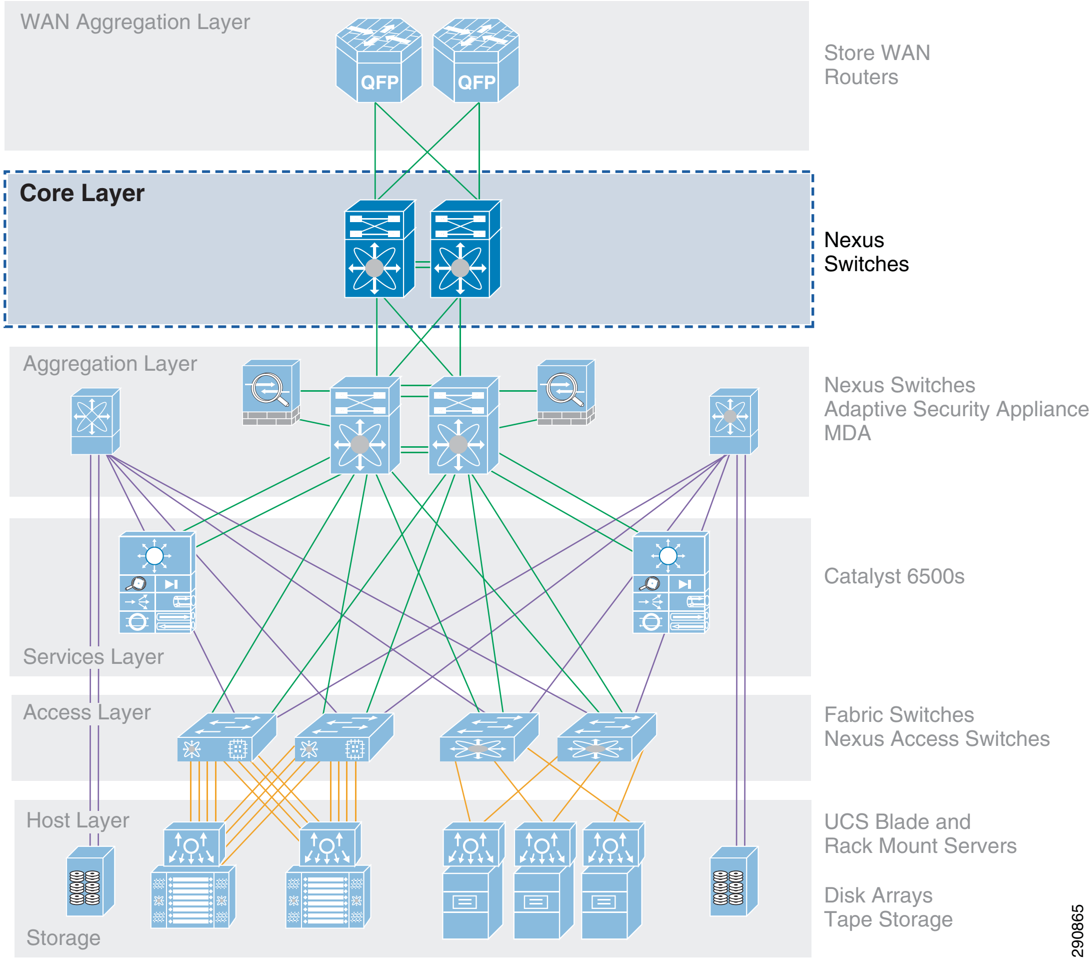
There are two typical WAN speeds categories for a WAN aggregation network: less than and up to OC3 (155 Mbps), and OC12 (622 Mbps) and above. The choice of these two network speeds determines the platform set to select from Cisco. In addition, this design creates two profiles for each WAN speed. These profiles are designed to provide guidance when designing a WAN edge network, regardless of which enterprise WAN architecture is selected. The profiles for each WAN speed investigate integrated versus dedicated chassis for each functionality component, as highlighted in the previous section. Some customers prefer a highly integrated solution where most, if not all, of the WAN edge functions described in this document reside on a single or very few network devices. Other customers prefer the granularity and scalability of these same functions separated across multiple network devices.

The WAN aggregation architecture is based on the *Infrastructure Protection and Security Service Integration Design for the Next Generation WAN Edge v 2.0*, which can be found at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/IPSNGWAN.html

Core Layer

The core layer provides the high-speed packet switching backplane for all flows going throughout of the data center, as shown in Figure 3-7.

Figure 3-7 Core Layer



Design Considerations

The core layer provides connectivity to multiple aggregation layers and provides a resilient Layer 3 routed fabric with no single point of failure. The core layer runs an interior routing protocol, such as Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP), and load balances traffic between the core and aggregation layers using the Cisco Express Forwarding-based hashing algorithms.

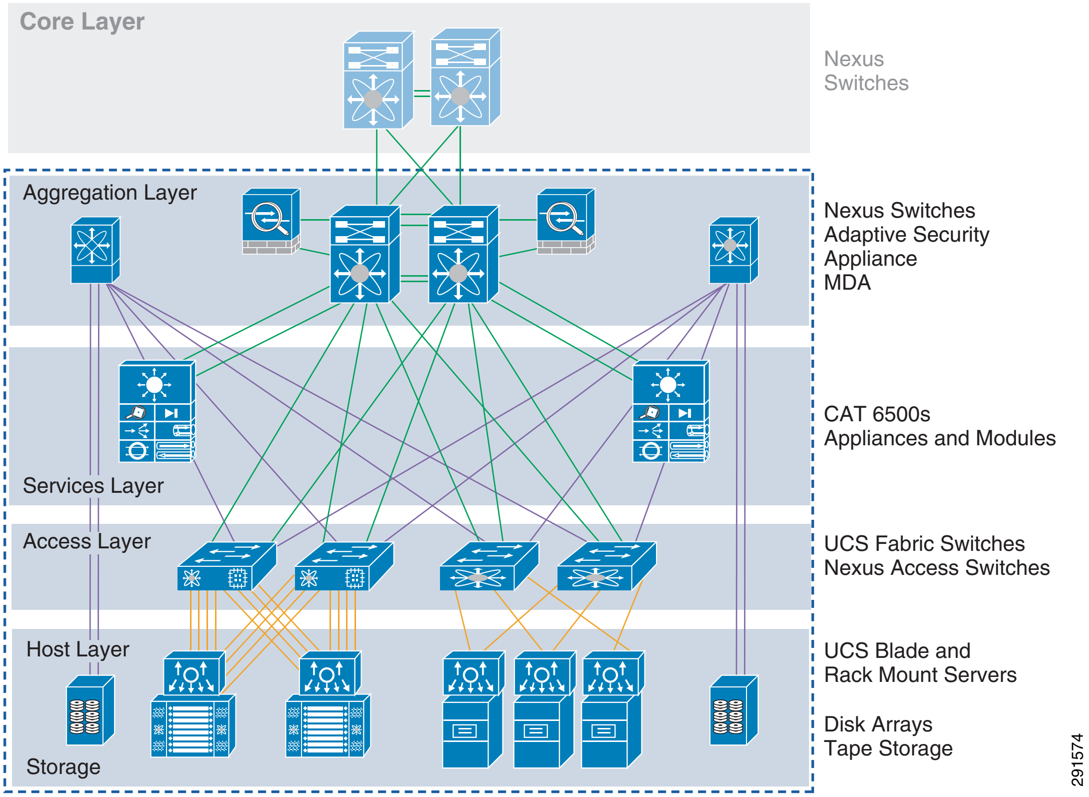
The core is not a perimeter; no security filtration should be performed at this layer.

The core, services aggregation, and server access tiers of the multi-tier data center architecture were based on the design documented in the *Cisco Data Center Infrastructure Design Guide 3.0*, which can be found at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/DC-3_0_IPInfra.html

Aggregation Block

An aggregation block is a combination of the aggregation, services, and access layer systems. It represents a repeatable, implementable template for scaling applications and services within the data center. (See Figure 3-8.)

Figure 3-8 Aggregation Block



Design Considerations

Zones are a best practice to isolate applications and services based on their individual policy requirements. You can securely mix in-scope and out-of-scope applications and services within a single aggregation block.

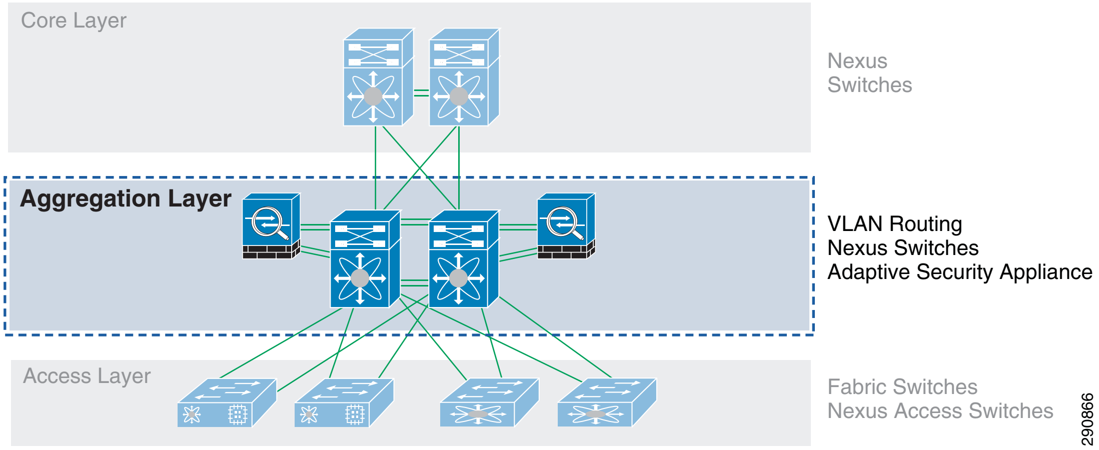
The layers that comprise the aggregation block are described in more detail below.

For more information, see the following URL:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns994/landing_aggregationlayer.html

Aggregation Layer

The aggregation layer aggregates the connections from the services layer and the access layer to the centralized core, as shown in Figure 3-9.

Figure 3-9 Aggregation Layer



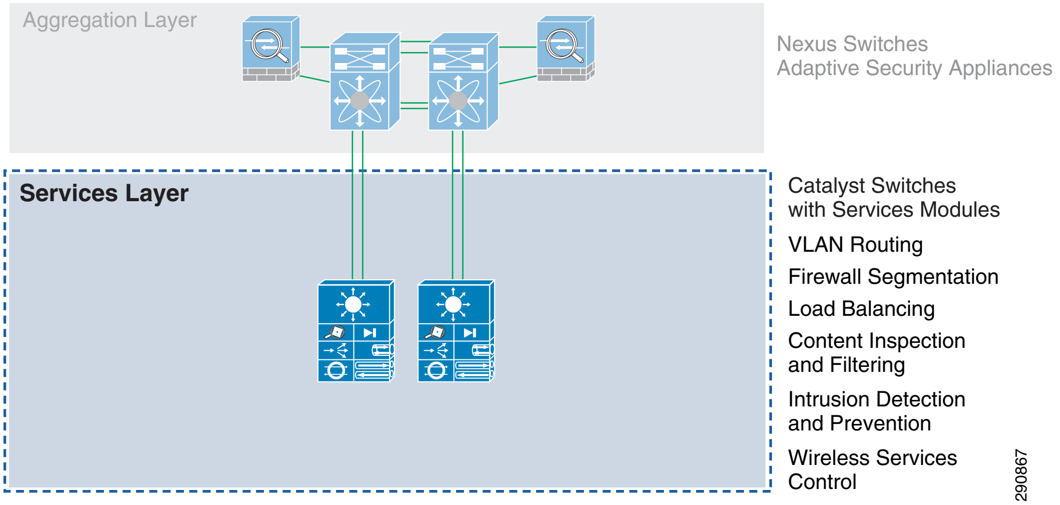
Design Considerations

The aggregation layer uses Layer 3 filters to segregate and protect the edge of the scope of compliance.

Services Layer

The services layer provides important functions, such as service module integration, Layer 2 domain definitions, spanning tree processing, and default gateway redundancy. (See Figure 3-10.)

Figure 3-10 Services Layer



Design Considerations

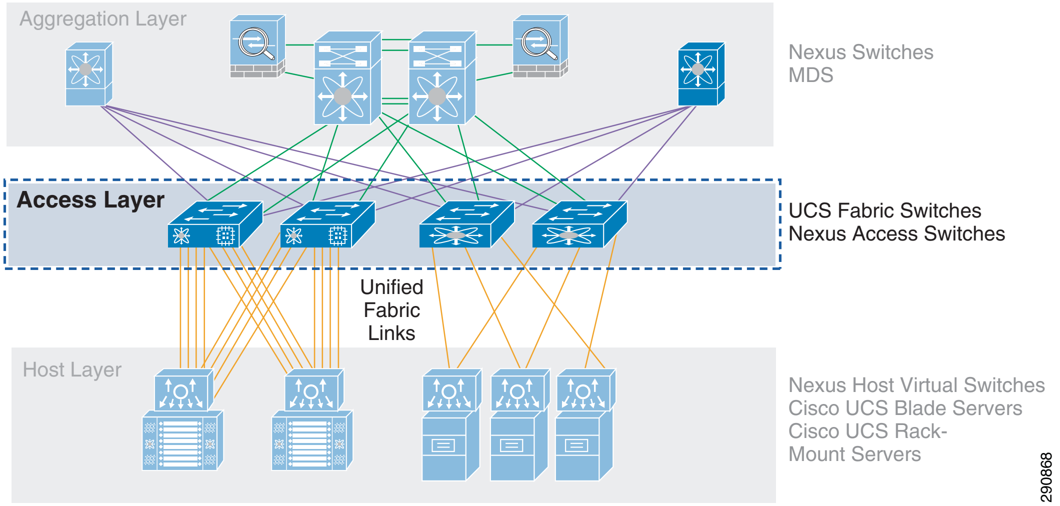
Services such as server load balancing and wide-area application services (WAAS) are used at this layer to optimize applications. Optimizing devices used within the scope of PCI are also brought into scope and are susceptible to the same controls as traditional network devices. For more information on understanding these controls, consult the capability assessment logic in Chapter 5, "Component Assessment."

Services such as content switching, SSL offload, intrusion detection, and network analysis are provided by hardware-based service modules or standalone appliances.

Access Layer

The access layer is where the servers physically attach to the network, as shown in Figure 3-11.

Figure 3-11 Access Layer



In typical data centers, the server components consist of appliances, 1RU servers, blade servers with integral switches, blade servers with pass-through cabling, clustered servers, and mainframes with OSA adapters. The access layer network infrastructure consists of modular switches, fixed configuration 1RU or 2RU switches, and integral blade server switches.

Design Considerations

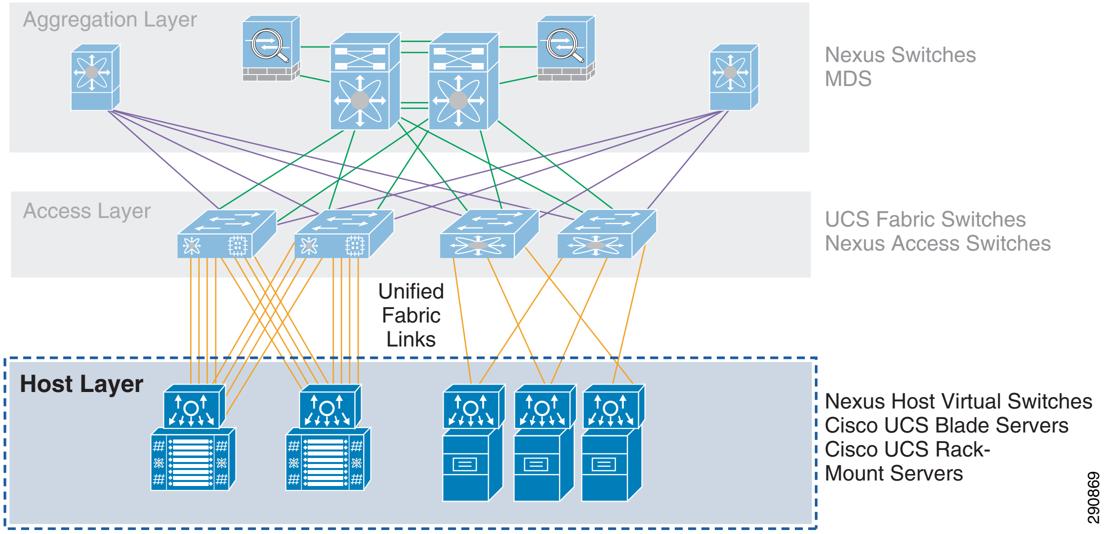
Switches provide both Layer 2 and Layer 3 topologies, fulfilling the various server broadcast domain or administrative requirements.

The solution management servers connect to the network in this layer. They are centralized, segmented from other business application servers, and protected by firewall services from the service aggregation layer above. Business servers, consisting of POS transaction log servers, database, and data warehouse servers also exist at this layer but are segmented via separate VLANs and firewall policy.

Host/Server Farm Layer

The host/server farm layer is where the centralized administrative applications reside, as shown in Figure 3-12.

Figure 3-12 Host/Server Farm Layer



Design Considerations

Network addressing should be used per business function. This allows the discrete manipulation of data traffic as requirements arise. For example, both POS applications and network management are used within the scope of PCI compliance but should be segregated onto their own subnets.

Virtualization technology can be used within a data center server farm. Individual blades within a blade server chassis can be used to segment sensitive and non-sensitive applications because they run independent hypervisors. Because hypervisors are considered insecure, when mixing sensitive applications with non-sensitive applications (mixed-mode) across the same hypervisor, the non-sensitive applications are now in scope.

For more information, see the PCI Virtualization Guidelines whitepaper at the following URL: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.

Multiple internal Network Time Protocol (NTP) servers should be deployed for consistent log synchronization in the event of failure. Those internal NTP servers should use more than one external source in the event of an external failure.

Although virtualization can be used for a variety of services, NTP requires a high resolution system clock and accurate response times to clock interrupts that virtual machines cannot provide. For these reasons, it is recommended not to run NTP on virtual machines. Instead, NTP should be run on the base OS of the hypervisor, and the virtual machine should use VMware Tools Clock synchronization to sync with the base host. NTP servers should also not run on virtual machines but on physical devices (for example, on the Cisco Catalyst 6509 Services switches in the services layer of the data center aggregation block). For more details, see the following URL: http://www.vmware.com/files/pdf/Timekeeping-In-VirtualMachines.pdf.

Table 3-2 lists descriptions of applications for administrators.

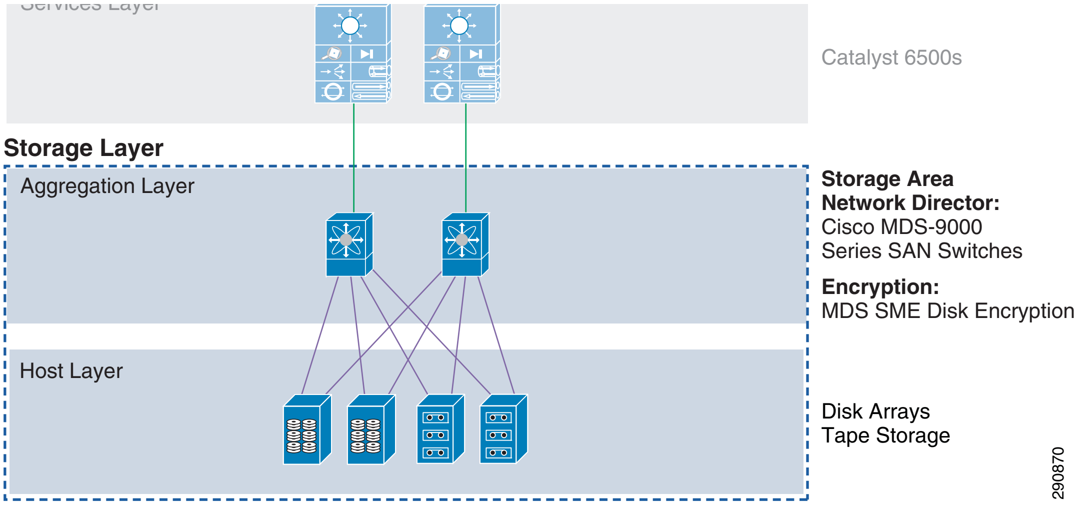
Table 3-2 Central Toolkit Description of Applications for Administrators

Function	Solution Component Options
Authentication	
Device AAA	Cisco Secure ACS, Cisco ISE
Two-factor remote	RSA Authentication Manager
Directory services	Active Directory
Network Management	
Device configuration	Cisco LMS, EMC Ionix NCM
Security configuration	Cisco Security Manager
Wireless configuration	Cisco WCS
Monitoring	
Event correlation	RSA enVision
Policy enforcement	EMC Ionix NCM
Corporate policy	RSA Archer
Virtualization	EMC Unified Infrastructure Manager, VMware vSphere
Physical Security	
Video surveillance	Cisco Video Surveillance Manager
Building access	Cisco Physical Access Manager
Encryption	
Storage	Cisco Key Manager, RSA Data Protection Manager
Remote access/VPN	Cisco Security Manager

Storage Layer

The storage layer is where sensitive data is stored, as shown in Figure 3-13.

Figure 3-13 Storage Layer



Design Considerations

A combination of disk encryption provided by Cisco MDS, Fibre-Channel zoning, and masking were used in the storage implementation of this solution. By deploying zoning within a Fibre Channel fabric, device access is limited to devices within the zone. This allows the user to segregate devices based on access to a particular storage device (disk array). This is a requirement in a data center environment in which multiple file servers in the data center server farm are connected to the same SAN fabric, and access to cardholder data must be restricted to a subset of servers. LUN masking takes zoning beyond the Fibre Channel switchport level, by restricting access to specific LUNs on a given disk array. Only specific devices belonging to the LUN zone are able to access those sections of the disk.

Encryption keys for storage are managed by Cisco Key Manager and RSA Data Protection Manager.

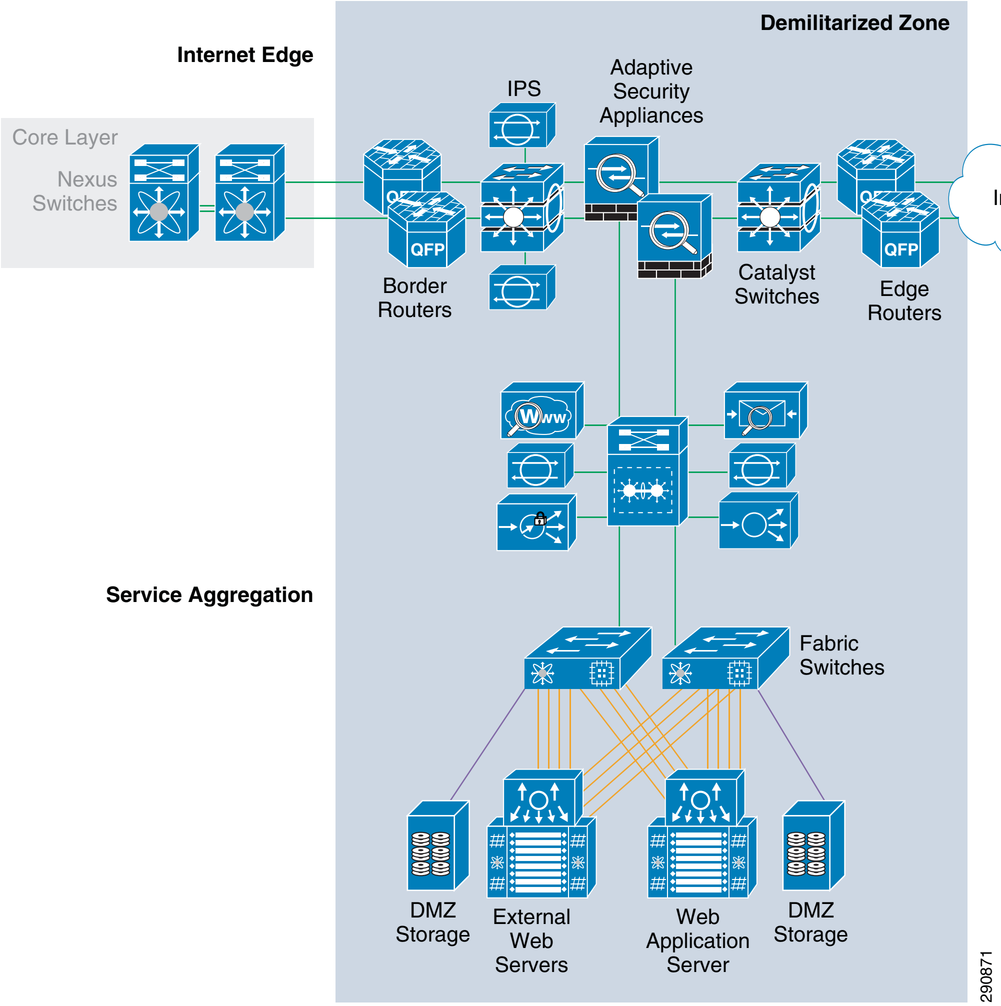
A subtle, yet potentially significant change to key management has been introduced with the PCI 2.0 standard. With past versions of the DSS, annual key rotations were required for encryption keys. DSS 2.0 now requires that keys are rotated at the end of their *cryptoperiod*, and references the NIST 800-57 Special Publication to determine what an appropriate cryptoperiod is. The NIST 800-57 Special Publication is a 324-page, three-part document. Merchants, and even QSAs, may not have the expertise to fully understand such a document that includes countless encryption scenarios, with cryptoperiods ranging from as short as a day to as long as three years.

In an ideal world, with all parties being expert cryptographers, this risk-based change to the standard would be very appropriate and most welcome. However, given the number of scenarios and criteria for determining an appropriate cryptoperiod, it could suggest that this change is too subjective and may become a point of contention between a merchant and QSA assessor, as to what is an appropriate cryptoperiod; whereas the former, more prescriptive control, did not allow for flexibility in this area.

E-commerce/Internet Edge/Service Provider Edge/Partner Edge

The solution uses a collapsed Internet edge and extranet network to support Internet connectivity and business partner connectivity, as shown in Figure 3-14.

Figure 3-14 E-commerce/Internet Edge/Service Provider Edge



Design Considerations

The design does the following:

- Provides an enterprise connection to the Internet
- Secures the Internet edge design using Cisco firewall and intrusion detection systems
- Provides a dual-threaded design for network resiliency
- Provides a collapsed Internet edge and extranet network for a highly centralized and integrated edge network
- Provides remote VPN access to enterprise users/telecommuters

This design takes into account best practices from the *Data Center Networking: Internet Edge Design Architecture Design Guide* (http://www.cisco.com/go/designzone) and customizes these recommendations for the Internet edge and extranet networks of retail businesses. The edges connect Internet services to the complete enterprise environment (that is, from headquarters to Internet service providers), and branch office connections that use a Cisco secure VPN to connect to headquarters. The collapsed design provides highly centralized and integrated edge networks, and transports the aggregated traffic through various service modules (Cisco ACE, Cisco FWSM, and Cisco IDSM2) within a pair of Cisco Catalyst 6500 Switch chassis. The Internet edge provides the following security functions:

- Secure configurations and management.
- IP anti-spoofing.
- Access control lists (ACLs) that provide explicitly permitted and/or denied IP traffic that may traverse between inside, outside, and DMZ.
- Stateful inspection provides the ability to establish and monitor session states of traffic permitted to flow across the Internet edge, and to deny traffic that fails to match the expected state of existing or allowed sessions.
- Intrusion detection using Cisco IDSM2 provides the ability to promiscuously monitor traffic across discrete points within the Internet edge, and to alarm and/or take action after detecting suspect behavior that may threaten the enterprise network.
- Applications servers that need to be directly accessed from the Internet are placed in a quasi-trusted secure area (DMZ) between the Internet and the internal enterprise network, which allows internal hosts and Internet hosts to communicate with servers in the DMZ.
- All public-facing web applications should be developed using the security best practices to prevent known attacks, and must be reviewed annually or after changes.

CHAPTER 4

Solution Implementation

Overview

Cisco customers have asked Cisco to provide insight into how Cisco products can be used to address PCI DSS 2.0 requirements. To fully accomplish this goal, Cisco hired an auditor and went through the same process as retailers. To audit Cisco products for the capability to address compliance, they had to be installed and configured within a representative design.

This chapter demonstrates how the Cisco PCI Solution for Retail was installed and configured to address the specifications of PCI 2.0. Cisco partnered with RSA, HyTrust, EMC, VCE, and Verizon Business to create a comprehensive design that reflected the framework and architectural principles discussed in earlier chapters.

The Cisco PCI Solution for Retail was validated in the Cisco Retail Lab in San Jose, California. The stores, data center, WAN, and Internet edge network infrastructures were built using Cisco best practice design guides, as represented by the Connected Retail Reference Architecture (http://www.cisco.com/go/designzone). The individual components were installed and configured to adhere to PCI 2.0 specifications. Verizon Business then conducted an assessment of the design and advised on remediation for specific configurations of individual components. After the remediation was complete, Verizon Business provided a detailed reference architecture report (see Appendix B, "Verizon Business Reference Architecture Report—Cisco PCI Solution for Retail.")

Tip An ***architecture*** is a strategic structure for the consistent design, construction, and operation of systems to achieve a desired set of outcomes.

A ***design*** is a tactical implementation of an architectural strategy, using specific configurations of products to satisfy business requirements.

Chapter 3, "Solution Architecture," describes the enterprise architecture with regards to compliance. This chapter demonstrates a design or, in other words, a specific implementation of components to achieve these principles. Various designs can result from the solution architecture. The design that was implemented is not intended to represent the only way that Cisco and partner products can be installed to address PCI. It is intended to provide an example showing how and what was used to achieve the principles described in Chapter 3, "Solution Architecture."

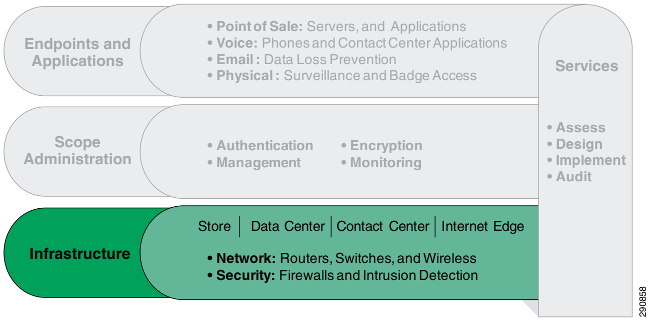
Although every company has specific considerations that vary from this implementation, these designs and the configurations of the components in Appendix E, "Detailed Full Running Configurations," provide an instructive example of what is needed to secure credit card data. Each component selected was audited for its capabilities, and that assessment is covered in the next chapter.

In each section, the reference architecture is shown with the corresponding design that was implemented and validated within the Cisco PCI laboratories. The full configurations of each individual component are available in Appendix E, "Detailed Full Running Configurations."

Infrastructure

The infrastructure layer of the solution framework addresses the components such as routers, switches, firewalls, and security components, as shown in Figure 4-1.

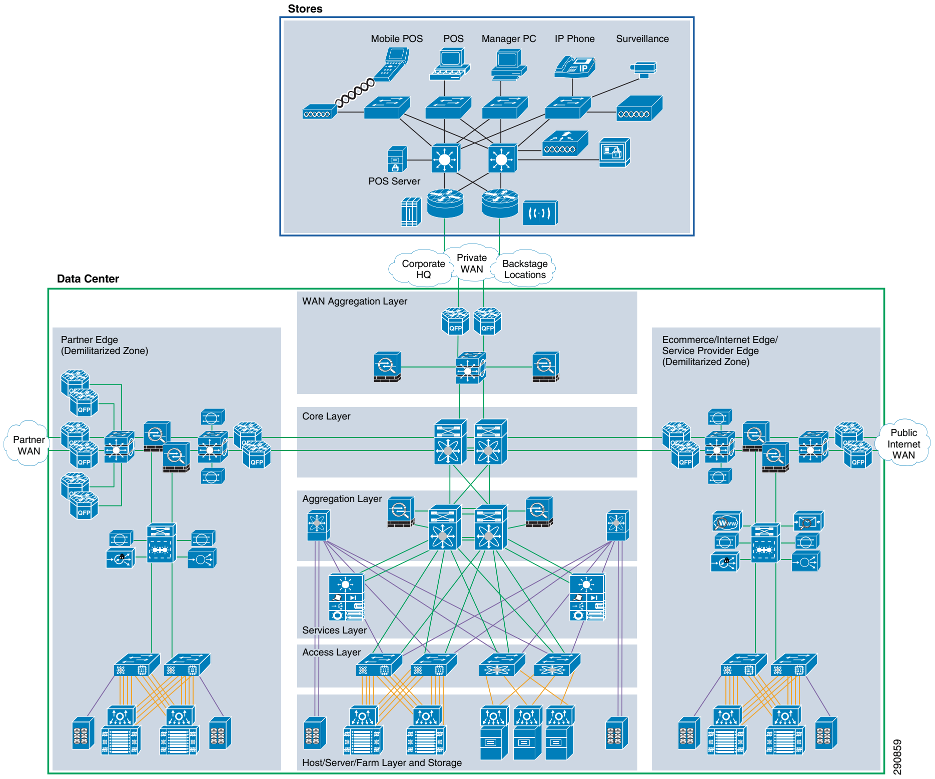
Figure 4-1 Infrastructure Layer of the Solution Framework


Endpoints and Applications
• Point of Sale: Servers, and Applications
• Voice: Phones and Contact Center Applications
• Email: Data Loss Prevention
• Physical: Surveillance and Badge Access
Services
Scope Administration
• Authentication
• Management
• Encryption
• Monitoring
• Assess
• Design
• Implement
• Audit
Infrastructure
Store
Data Center
Contact Center
Internet Edge
• Network: Routers, Switches, and Wireless
• Security: Firewalls and Intrusion Detection
290858

The following sections describe the designs that were implemented from the reference architecture.

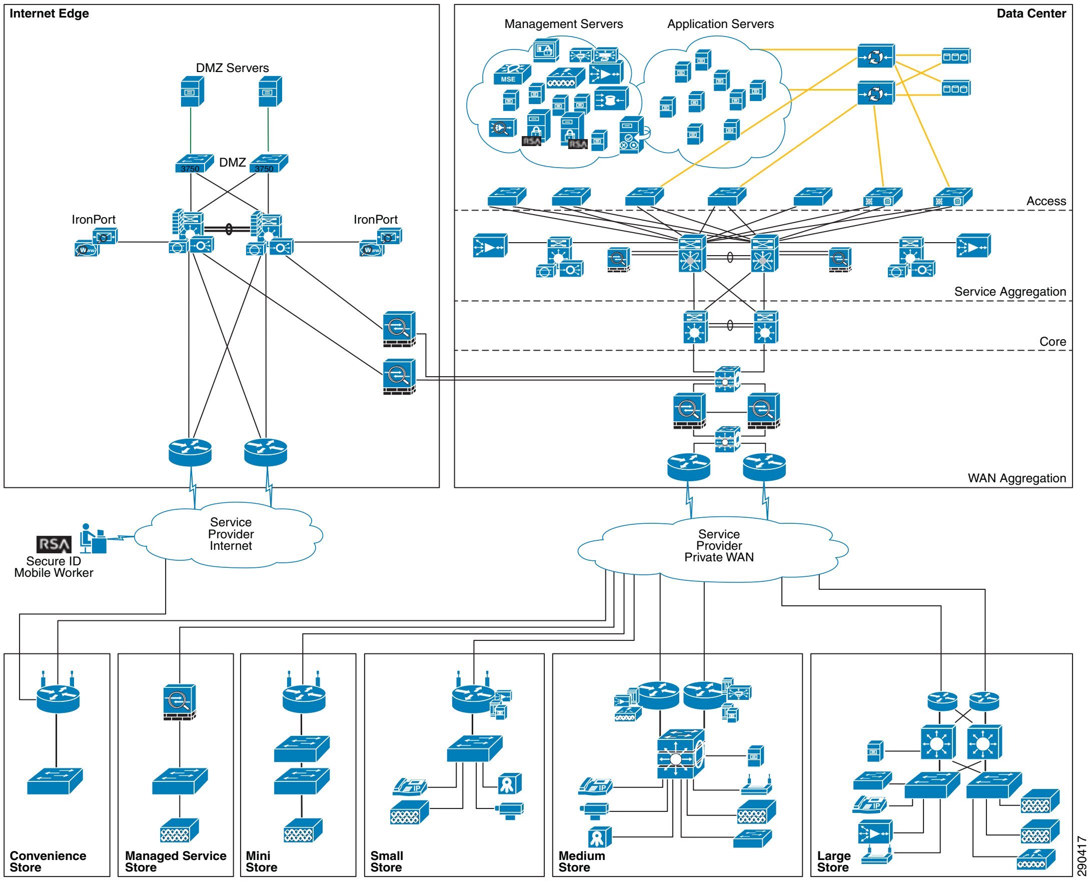
Figure 4-2 shows the retail enterprise-wide reference architecture.

Figure 4-2 Retail Enterprise-Wide Reference Architecture



Referencing the retail enterprise-wide architecture shown in Figure 4-2, the design shown in Figure 4-3 was created in the Cisco Retail Lab.

Figure 4-3 Cisco PCI Solution for Retail Lab Architecture



Note the following:

- Six store designs were selected to represent Cisco and partner products.
- The data center consists of a single aggregation block based on the Data Center 3.0 architecture.
- The Internet edge is representative of both the e-commerce and partner edge for the purposes of validation.

The following sections describe this enterprise-wide design in more detail, and demonstrate what was implemented within the lab.

Stores

Multiple store footprints were implemented that address a variety of business objectives. Each store footprint section contains designs that were extracted from the reference architecture. Each design contains the following:

- Reference architecture
- Store design
  - Logical topology
  - Addressing plan
  - Components selected

For component compliance functionality, see Chapter 5, "Component Assessment.". For full device configurations, see Appendix E, "Detailed Full Running Configurations."

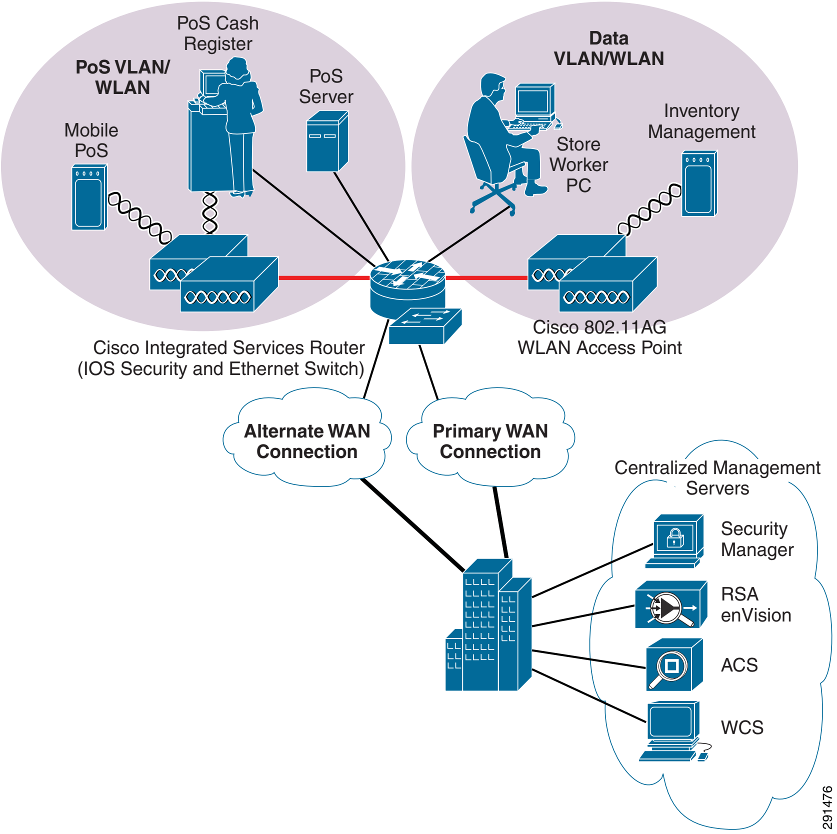
Note Each of these store designs includes a variety of components that can be interchangeably used between them, depending on business requirements. For validation purposes, it was not necessary to implement all possible components in each design.

Small Store Architecture

The small store network scenario, shown in Figure 4-4, meets the following design requirements:

- Store size averages between 2000–6000 square feet
- Fewer than 25 devices requiring network connectivity
- Single router with firewall/IPS, integrated Ethernet switch, compact switch, and power-over-Ethernet (PoE)
- Preference for integrated services within fewer network components because of physical space requirements
- Wireless connectivity

Figure 4-4 Small Store Architecture



The small store reference architecture is a powerful platform for running an enterprise retail business that requires simplicity and a compact form factor. This combination appeals to many retail formats that can include the following:

- Small store—Specialty shops, discount retailers
- Mini stores—Fuel stations, mall outlet
- Convenience stores—Pop-up stores, mall kiosks
- Managed service provider store—WAN access controlled by service provider

This network architecture is widely used and consolidates many services into fewer infrastructure components. The small store also supports a variety of retail business application models because an integrated Ethernet switch supports high-speed LAN services. In addition, an integrated content engine supports centralized application optimization requirements such as Web Cache Communications Protocol (WCCP)-based caching, pre-positioning of data, local media streaming, and other application velocity services.

Advantages include the following:

- Lower cost per store
- Fewer parts to spare
- Fewer software images to maintain
- Lower equipment maintenance costs

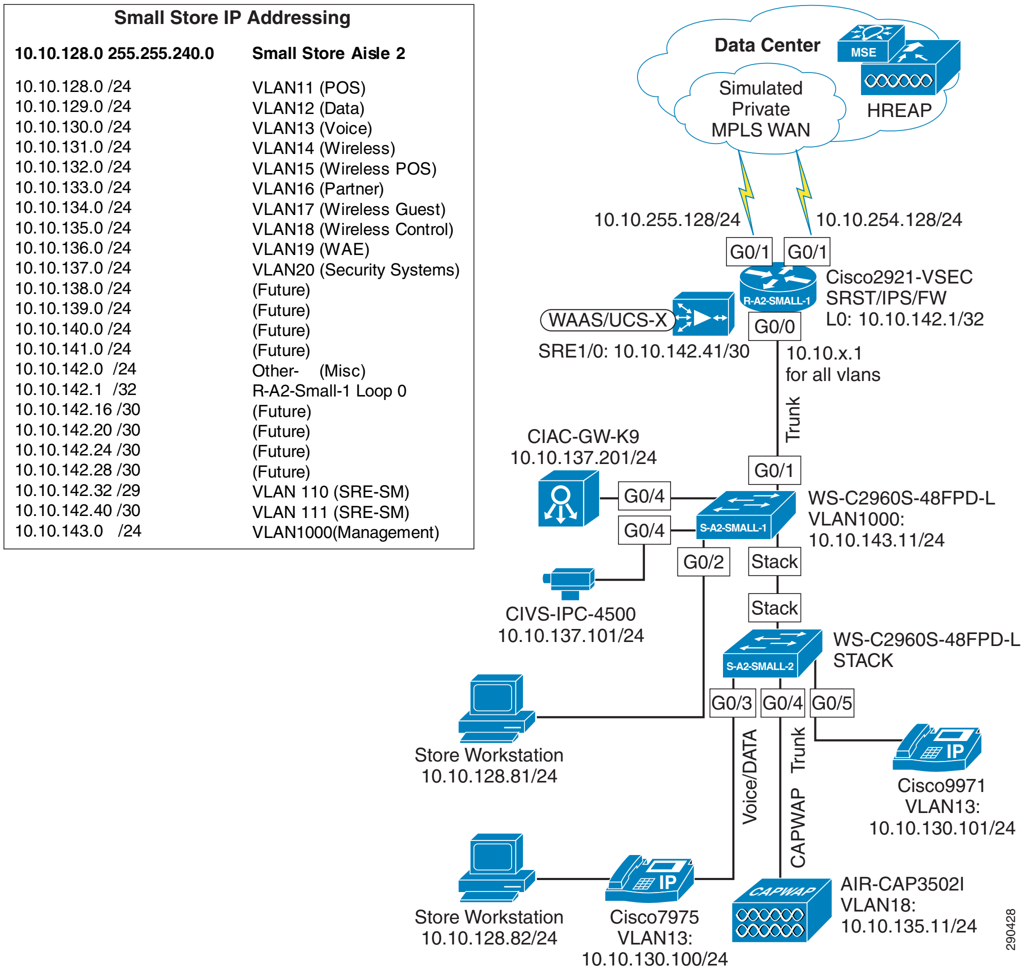
Limitations include the following:

- Decreased levels of network resilience
- Greater potential downtime because of single points of failure

Small Store—Small Design

Figure 4-5 shows the small store network design.

Figure 4-5 Small Store Network Design



Small Store IP Addressing

10.10.128.0 255.255.240.0	Small Store Aisle 2
10.10.128.0 /24	VLAN11 (POS)
10.10.129.0 /24	VLAN12 (Data)
10.10.130.0 /24	VLAN13 (Voice)
10.10.131.0 /24	VLAN14 (Wireless)
10.10.132.0 /24	VLAN15 (Wireless POS)
10.10.133.0 /24	VLAN16 (Partner)
10.10.134.0 /24	VLAN17 (Wireless Guest)
10.10.135.0 /24	VLAN18 (Wireless Control)
10.10.136.0 /24	VLAN19 (WAE)
10.10.137.0 /24	VLAN20 (Security Systems)
10.10.138.0 /24	(Future)
10.10.139.0 /24	(Future)
10.10.140.0 /24	(Future)
10.10.141.0 /24	(Future)
10.10.142.0 /24	Other- (Misc)
10.10.142.1 /32	R-A2-Small-1 Loop 0
10.10.142.16 /30	(Future)
10.10.142.20 /30	(Future)
10.10.142.24 /30	(Future)
10.10.142.28 /30	(Future)
10.10.142.32 /29	VLAN 110 (SRE-SM)
10.10.142.40 /30	VLAN 111 (SRE-SM)
10.10.143.0 /24	VLAN1000(Management)

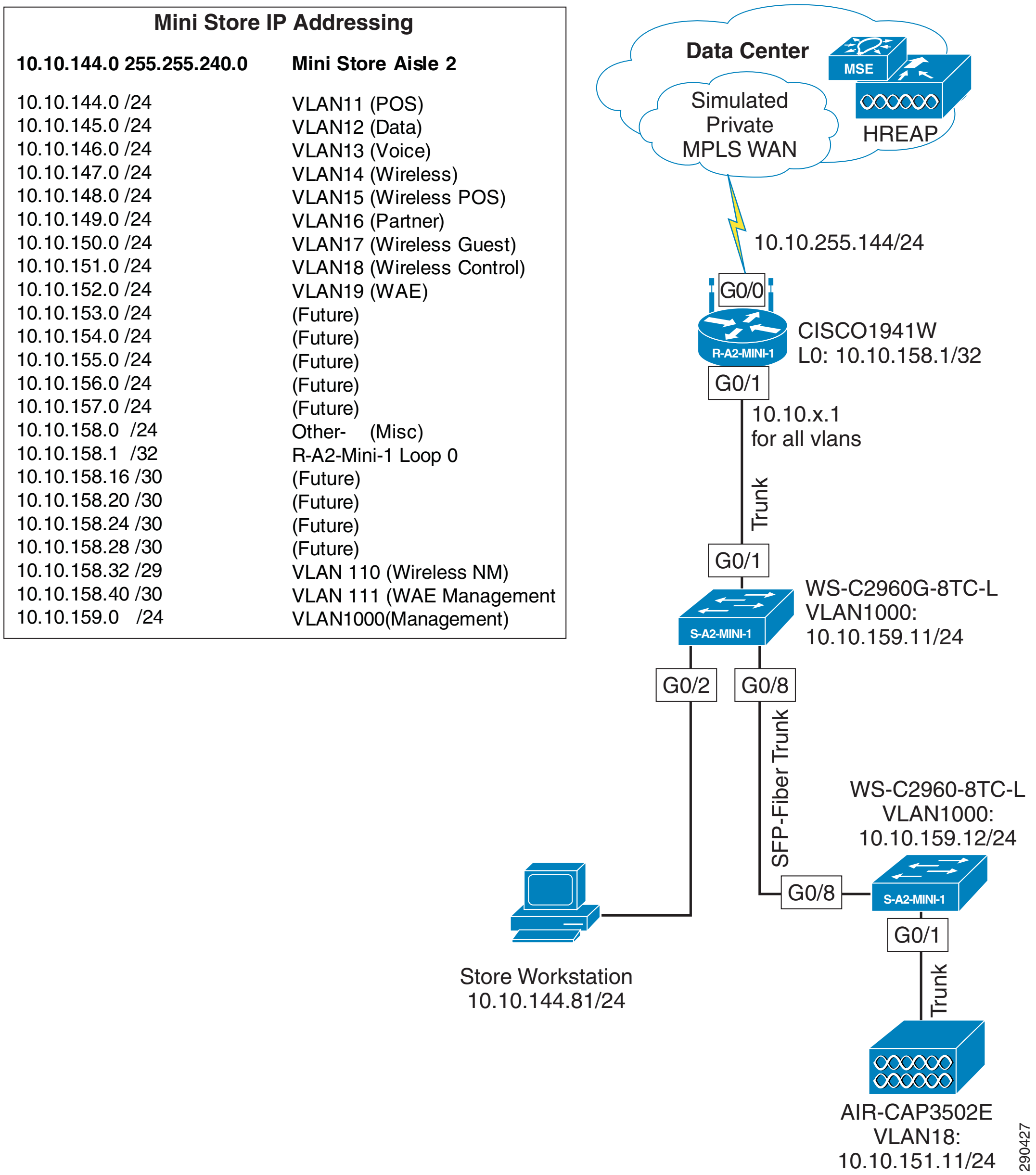
Components Selected

- Cisco 2921 Integrated Services Router (ISR)
- Cisco Catalyst 2960S 48-port PoE Switch
- Cisco Aironet 3502i Access Points
- Cisco Video Surveillance 4500 Series IP Cameras
- Cisco Physical Access Gateway

Small Store—Mini Design

The mini store represents an alternate design for the small store architecture, using different components. Figure 4-6 shows the mini store network design.

Figure 4-6 Mini Store Network Design



Mini Store IP Addressing

10.10.144.0 255.255.240.0	Mini Store Aisle 2
10.10.144.0 /24	VLAN11 (POS)
10.10.145.0 /24	VLAN12 (Data)
10.10.146.0 /24	VLAN13 (Voice)
10.10.147.0 /24	VLAN14 (Wireless)
10.10.148.0 /24	VLAN15 (Wireless POS)
10.10.149.0 /24	VLAN16 (Partner)
10.10.150.0 /24	VLAN17 (Wireless Guest)
10.10.151.0 /24	VLAN18 (Wireless Control)
10.10.152.0 /24	VLAN19 (WAE)
10.10.153.0 /24	(Future)
10.10.154.0 /24	(Future)
10.10.155.0 /24	(Future)
10.10.156.0 /24	(Future)
10.10.157.0 /24	(Future)
10.10.158.0 /24	Other- (Misc)
10.10.158.1 /32	R-A2-Mini-1 Loop 0
10.10.158.16 /30	(Future)
10.10.158.20 /30	(Future)
10.10.158.24 /30	(Future)
10.10.158.28 /30	(Future)
10.10.158.32 /29	VLAN 110 (Wireless NM)
10.10.158.40 /30	VLAN 111 (WAE Management
10.10.159.0 /24	VLAN1000(Management)

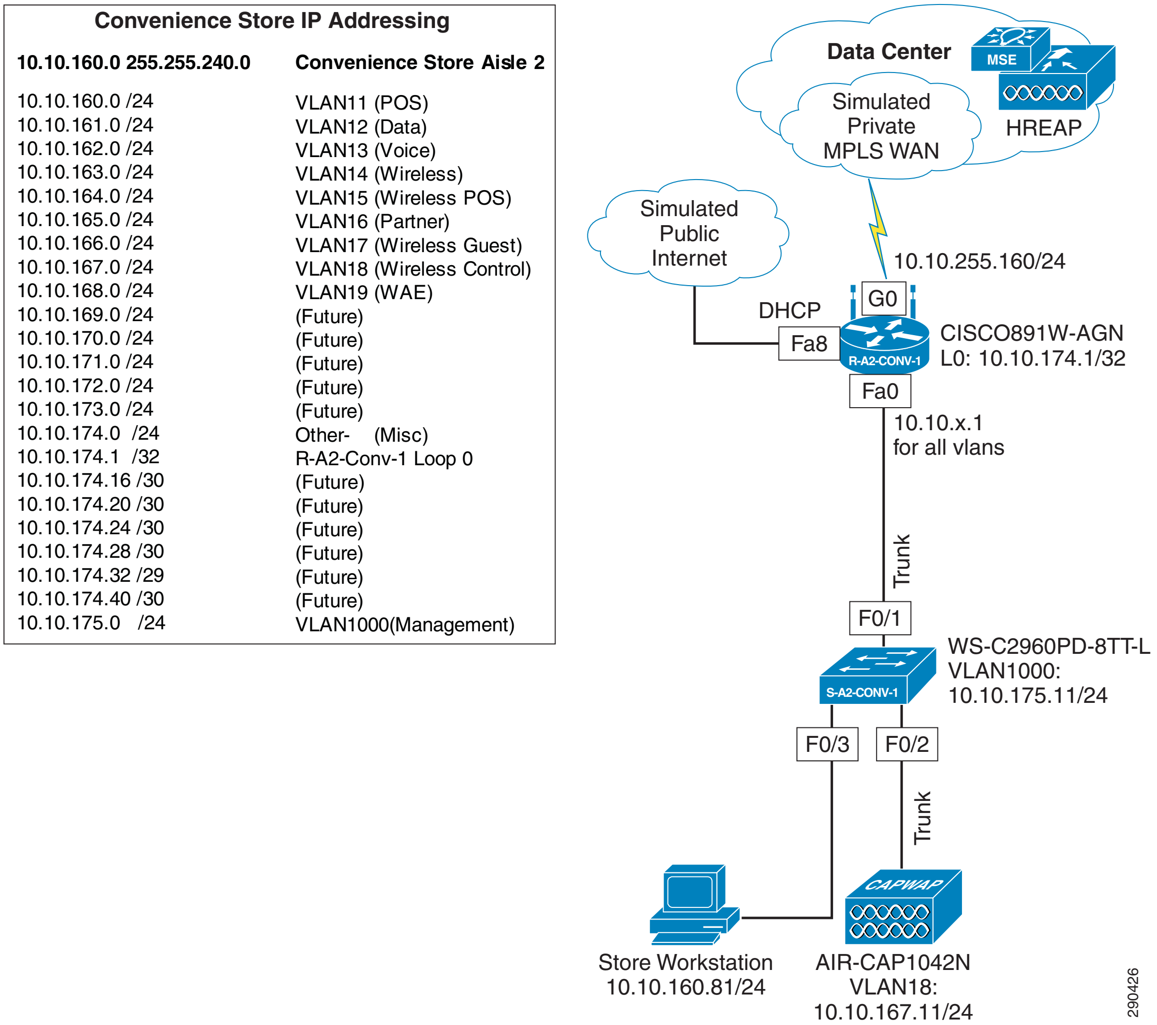
Components Selected

- Cisco 1941 Integrated Services Router (ISR)
- Cisco Catalyst 2960 Switch
- Cisco Aironet 3502e Access Point

Small Store—Convenience Design

The convenience store represents an alternate design for the small store architecture. Figure 4-7 shows the convenience store network design.

Figure 4-7 Convenience Store Network Design



Convenience Store IP Addressing

10.10.160.0 255.255.240.0	Convenience Store Aisle 2
10.10.160.0 /24	VLAN11 (POS)
10.10.161.0 /24	VLAN12 (Data)
10.10.162.0 /24	VLAN13 (Voice)
10.10.163.0 /24	VLAN14 (Wireless)
10.10.164.0 /24	VLAN15 (Wireless POS)
10.10.165.0 /24	VLAN16 (Partner)
10.10.166.0 /24	VLAN17 (Wireless Guest)
10.10.167.0 /24	VLAN18 (Wireless Control)
10.10.168.0 /24	VLAN19 (WAE)
10.10.169.0 /24	(Future)
10.10.170.0 /24	(Future)
10.10.171.0 /24	(Future)
10.10.172.0 /24	(Future)
10.10.173.0 /24	(Future)
10.10.174.0 /24	Other- (Misc)
10.10.174.1 /32	R-A2-Conv-1 Loop 0
10.10.174.16 /30	(Future)
10.10.174.20 /30	(Future)
10.10.174.24 /30	(Future)
10.10.174.28 /30	(Future)
10.10.174.32 /29	(Future)
10.10.174.40 /30	(Future)
10.10.175.0 /24	VLAN1000(Management)

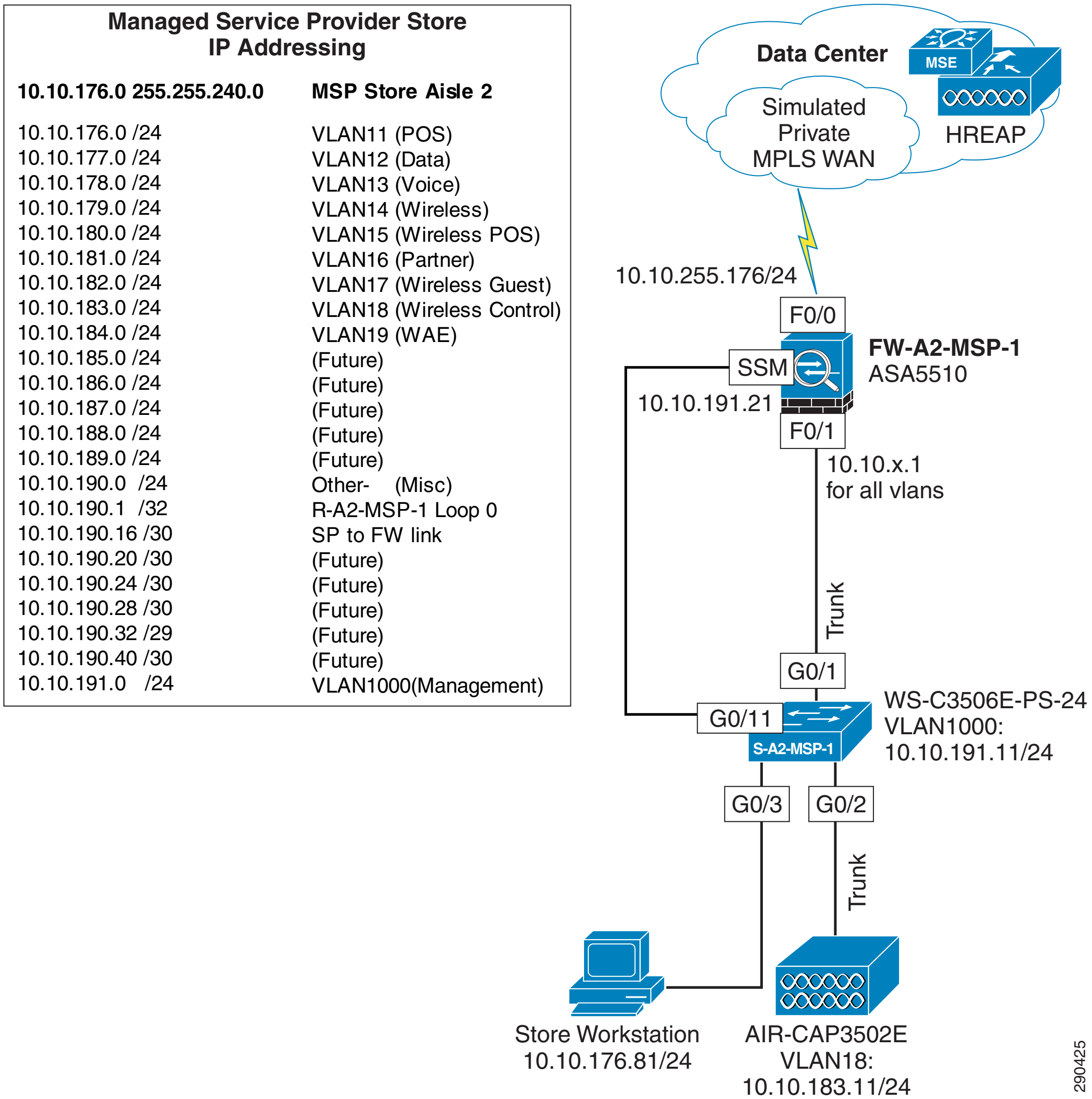
Components Selected

- Cisco 891 Series Integrated Services Router (ISR)
- Cisco Catalyst 2960 Series Switch
- Cisco Aironet 1042N Access Point

Small Store—Managed Service Provider Design

The managed service provider store represents an alternate design for the small store architecture. Figure 4-8 shows the managed service provider network design.

Figure 4-8 Managed Service Provider Network Design



Managed Service Provider Store IP Addressing

10.10.176.0 255.255.240.0	MSP Store Aisle 2
10.10.176.0 /24	VLAN11 (POS)
10.10.177.0 /24	VLAN12 (Data)
10.10.178.0 /24	VLAN13 (Voice)
10.10.179.0 /24	VLAN14 (Wireless)
10.10.180.0 /24	VLAN15 (Wireless POS)
10.10.181.0 /24	VLAN16 (Partner)
10.10.182.0 /24	VLAN17 (Wireless Guest)
10.10.183.0 /24	VLAN18 (Wireless Control)
10.10.184.0 /24	VLAN19 (WAE)
10.10.185.0 /24	(Future)
10.10.186.0 /24	(Future)
10.10.187.0 /24	(Future)
10.10.188.0 /24	(Future)
10.10.189.0 /24	(Future)
10.10.190.0 /24	Other- (Misc)
10.10.190.1 /32	R-A2-MSP-1 Loop 0
10.10.190.16 /30	SP to FW link
10.10.190.20 /30	(Future)
10.10.190.24 /30	(Future)
10.10.190.28 /30	(Future)
10.10.190.32 /29	(Future)
10.10.190.40 /30	(Future)
10.10.191.0 /24	VLAN1000(Management)

Components Selected

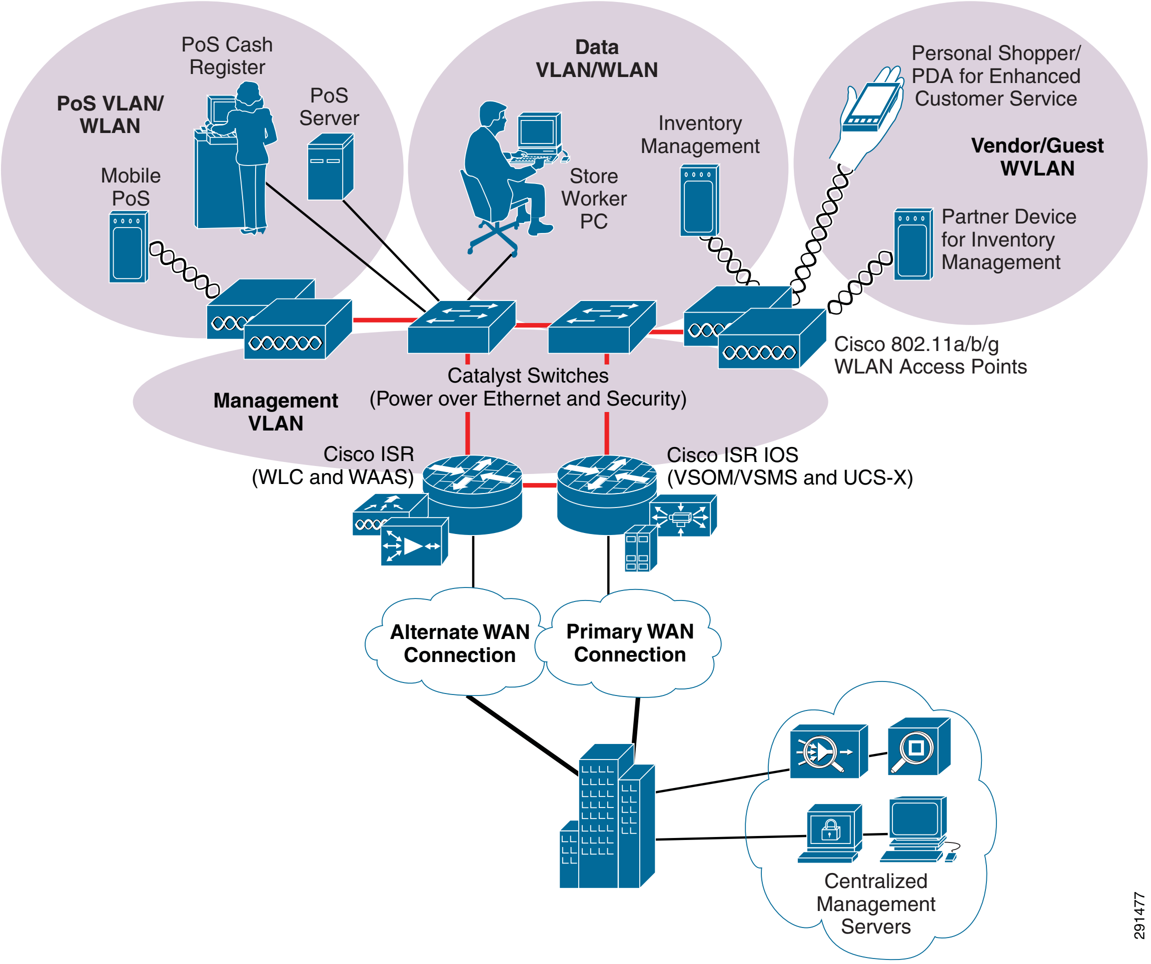
- Cisco ASA 5510 Firewall with SSM-10
- Cisco Catalyst 3560E Switch
- Cisco Aironet 3502e Access Points

Medium Store Architecture

The medium store network scenario, shown in Figure 4-9, meets the following design requirements:

- Store size averages between 6,000–18,000 square feet
- The physical size of the store is smaller than a large store, so a distribution layer of network switches is not required
- Number of devices connecting to the network averages 25–100 devices
- Redundant LAN and WAN infrastructures with firewall/IPS
- Wireless connectivity

Figure 4-9 Medium Store Architecture


PoS Cash Register
PoS VLAN/ WLAN
PoS Server
Mobile PoS
Data VLAN/WLAN
Inventory Management
Store Worker PC
Personal Shopper/ PDA for Enhanced Customer Service
Vendor/Guest WVLAN
Partner Device for Inventory Management
Cisco 802.11a/b/g WLAN Access Points
Catalyst Switches (Power over Ethernet and Security)
Management VLAN
Cisco ISR (WLC and WAAS)
Cisco ISR IOS (VSOM/VSMS and UCS-X)
Alternate WAN Connection
Primary WAN Connection
Centralized Management Servers
291477

The medium retail store reference architecture is designed for enterprise retail businesses that require network resilience and increased levels of application availability over the small store architecture and its single-threaded, simple approach. As more mission-critical applications and services converge onto the IP infrastructure, network uptime and application availability are more important. The dual-router and dual-LAN switch design of the medium store supports these requirements. Each of the Cisco ISR routers can run Cisco IOS Software security services and other store communication services simultaneously. Each of the Cisco ISR routers is connected to a dedicated WAN connection. Hot Standby Routing Protocol (HSRP) is used to ensure network resilience in the event that the network connection fails.

The access layer of the network offers enhanced levels of flexibility and more access ports compared to the small store. Up to 12 wireless access points can be installed in the store, supported by the Cisco Wireless Control System (WCS) controller as tested and without adding more controllers. The distributed Cisco Catalyst switches can support a combination of larger physical buildings or a larger number of endpoints than the small store.

Advantages include the following:

- More adaptive access layer with support for a greater number of endpoints and more diverse building requirements (multiple floors, sub-areas, and so on)
- Improved network resilience through parallel device design
- Improved network and application availability through parallel paths

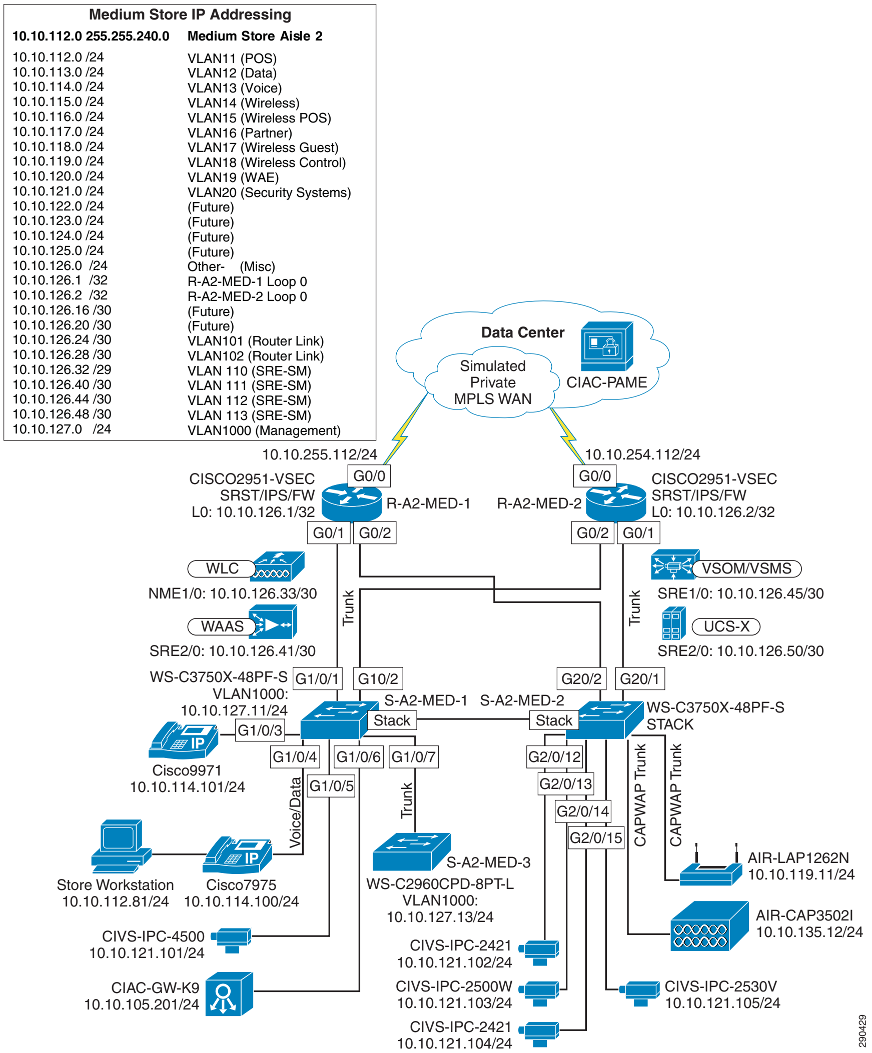
Limitations include the following:

- No distribution layer between core layer (the ISR) and the access layer switches
- Single WCS Controller decreases in-store resilience of the wireless network; the recommendation is to have store APs fallback to the central WCS controller if the local WCS controller fails, or to install dual-local WCS controllers.

Medium Store—Design

Figure 4-10 shows the medium store network design.

Figure 4-10 Medium Store Network Design



Medium Store IP Addressing

10.10.112.0 255.255.240.0	Medium Store Aisle 2
10.10.112.0 /24	VLAN11 (POS)
10.10.113.0 /24	VLAN12 (Data)
10.10.114.0 /24	VLAN13 (Voice)
10.10.115.0 /24	VLAN14 (Wireless)
10.10.116.0 /24	VLAN15 (Wireless POS)
10.10.117.0 /24	VLAN16 (Partner)
10.10.118.0 /24	VLAN17 (Wireless Guest)
10.10.119.0 /24	VLAN18 (Wireless Control)
10.10.120.0 /24	VLAN19 (WAE)
10.10.121.0 /24	VLAN20 (Security Systems)
10.10.122.0 /24	(Future)
10.10.123.0 /24	(Future)
10.10.124.0 /24	(Future)
10.10.125.0 /24	(Future)
10.10.126.0 /24	Other- (Misc)
10.10.126.1 /32	R-A2-MED-1 Loop 0
10.10.126.2 /32	R-A2-MED-2 Loop 0
10.10.126.16 /30	(Future)
10.10.126.20 /30	(Future)
10.10.126.24 /30	VLAN101 (Router Link)
10.10.126.28 /30	VLAN102 (Router Link)
10.10.126.32 /29	VLAN 110 (SRE-SM)
10.10.126.40 /30	VLAN 111 (SRE-SM)
10.10.126.44 /30	VLAN 112 (SRE-SM)
10.10.126.48 /30	VLAN 113 (SRE-SM)
10.10.127.0 /24	VLAN1000 (Management)

Components Selected

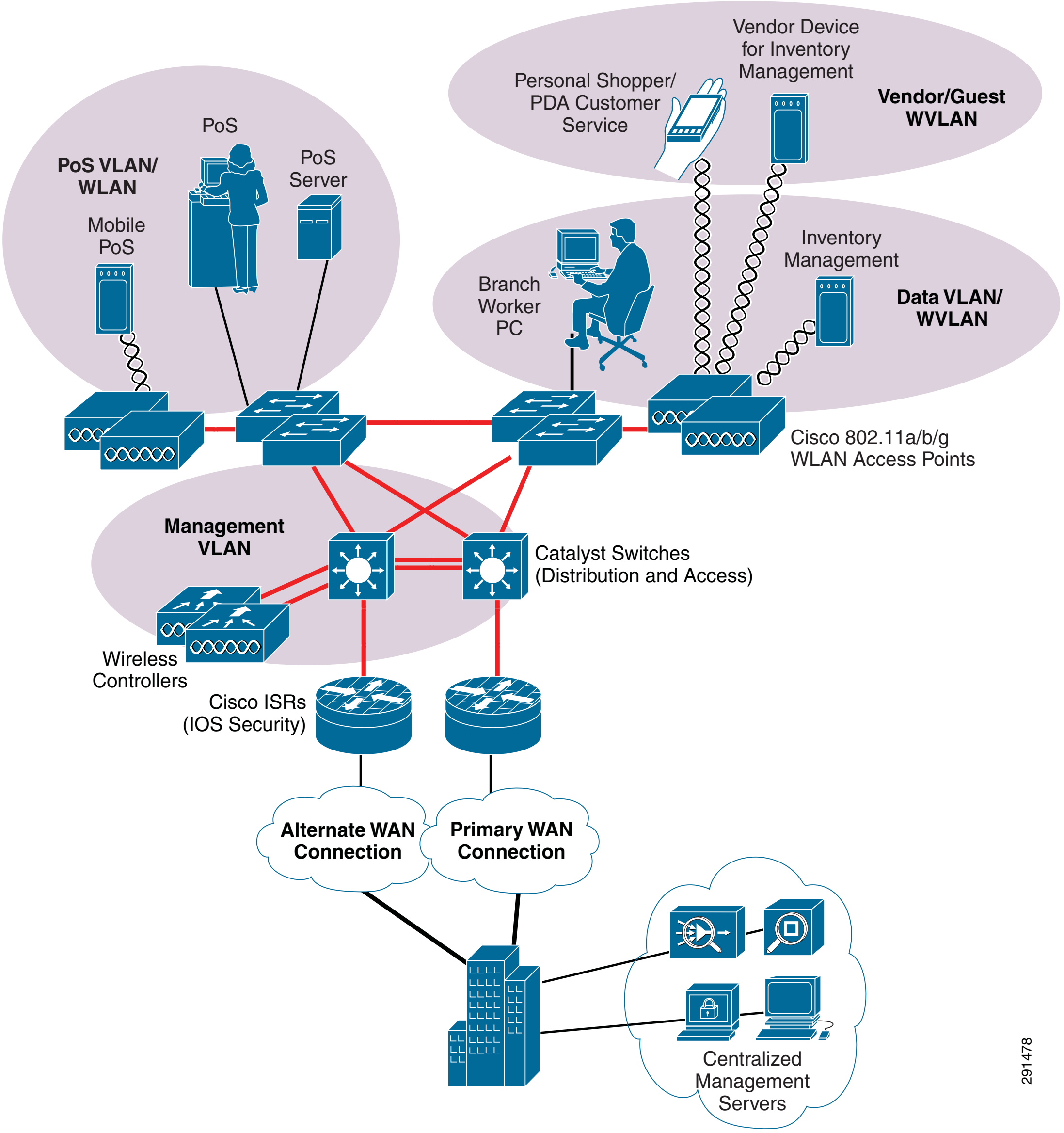
- Cisco 2951 Integrated Services Router (ISR)
- Cisco Catalyst 3750X 48-port PoE Switch
- Cisco Catalyst 2960 Compact Switch
- Cisco Aironet 3502e and 1262N Access Points
- Cisco Video Surveillance 2421 IP Dome Camera
- Cisco Video Surveillance 2500 Series IP Camera
- Cisco Operations Manager v4.1
- Cisco Physical Access Gateway

Large Store Architecture

The large store network scenario, shown in Figure 4-11, meets the following design requirements:

- Store size averages between 15,000–150,000 square feet
- More than 100 devices per store requiring network connectivity
- Multiple routers with firewall/IPS for primary and backup network requirements
- Preference for a combination of network services distributed within the store to meet resilience and application availability requirements
- Tiered network architecture within the store; distribution layer switches are employed between the central network services core and the access layer connecting to the network endpoints (POS, wireless APs, servers)

Figure 4-11 Large Store Architecture



The large retail store reference architecture takes some of the elements of Cisco campus network architecture recommendations and adapts them to a large retail store environment. Network traffic can be better segmented (logically and physically) to meet business requirements. The distribution layer of the large store architecture can greatly improve LAN performance while offering enhanced physical media connections (that is, fiber and copper for connection to remote access layer switches and wireless access points). A larger number of endpoints can be added to the network to meet business requirements. This type of architecture is widely used by large format retailers globally. Dual routers and distribution layer media flexibility greatly improve network serviceability because the network is highly available and scales to support the large retail store requirements. Routine maintenance and upgrades can be scheduled and performed more frequently or during normal business hours because of parallel path design.

Advantages include the following:

- Highest network resilience based on highly available design
- Port density and fiber density for large retail locations
- Increase segmentation of traffic
- Scalable to accommodate shifting requirements in large retail stores

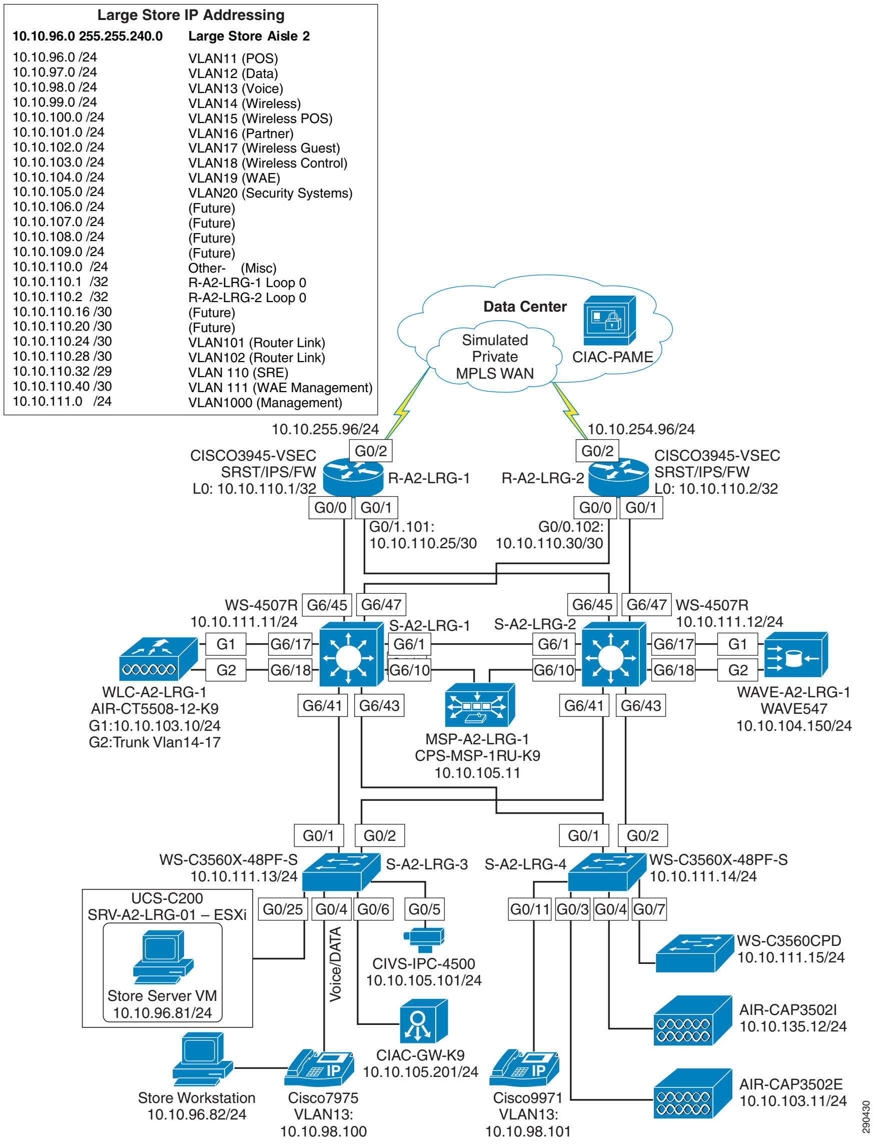
Limitations include the following:

- Higher cost because of network resilience based on highly available design
- These retail store network designs are capable of helping a retailer achieve PCI compliance, and also serve as the scalable platform for new services and applications

Large Store Design

Figure 4-12 shows the large store network design.

Figure 4-12 Large Store Network Design



Large Store IP Addressing

10.10.96.0 255.255.240.0	Large Store Aisle 2
10.10.96.0 /24	VLAN11 (POS)
10.10.97.0 /24	VLAN12 (Data)
10.10.98.0 /24	VLAN13 (Voice)
10.10.99.0 /24	VLAN14 (Wireless)
10.10.100.0 /24	VLAN15 (Wireless POS)
10.10.101.0 /24	VLAN16 (Partner)
10.10.102.0 /24	VLAN17 (Wireless Guest)
10.10.103.0 /24	VLAN18 (Wireless Control)
10.10.104.0 /24	VLAN19 (WAE)
10.10.105.0 /24	VLAN20 (Security Systems)
10.10.106.0 /24	(Future)
10.10.107.0 /24	(Future)
10.10.108.0 /24	(Future)
10.10.109.0 /24	(Future)
10.10.110.0 /24	Other- (Misc)
10.10.110.1 /32	R-A2-LRG-1 Loop 0
10.10.110.2 /32	R-A2-LRG-2 Loop 0
10.10.110.16 /30	(Future)
10.10.110.20 /30	(Future)
10.10.110.24 /30	VLAN101 (Router Link)
10.10.110.28 /30	VLAN102 (Router Link)
10.10.110.32 /29	VLAN 110 (SRE)
10.10.110.40 /30	VLAN 111 (WAE Management)
10.10.111.0 /24	VLAN1000 (Management)

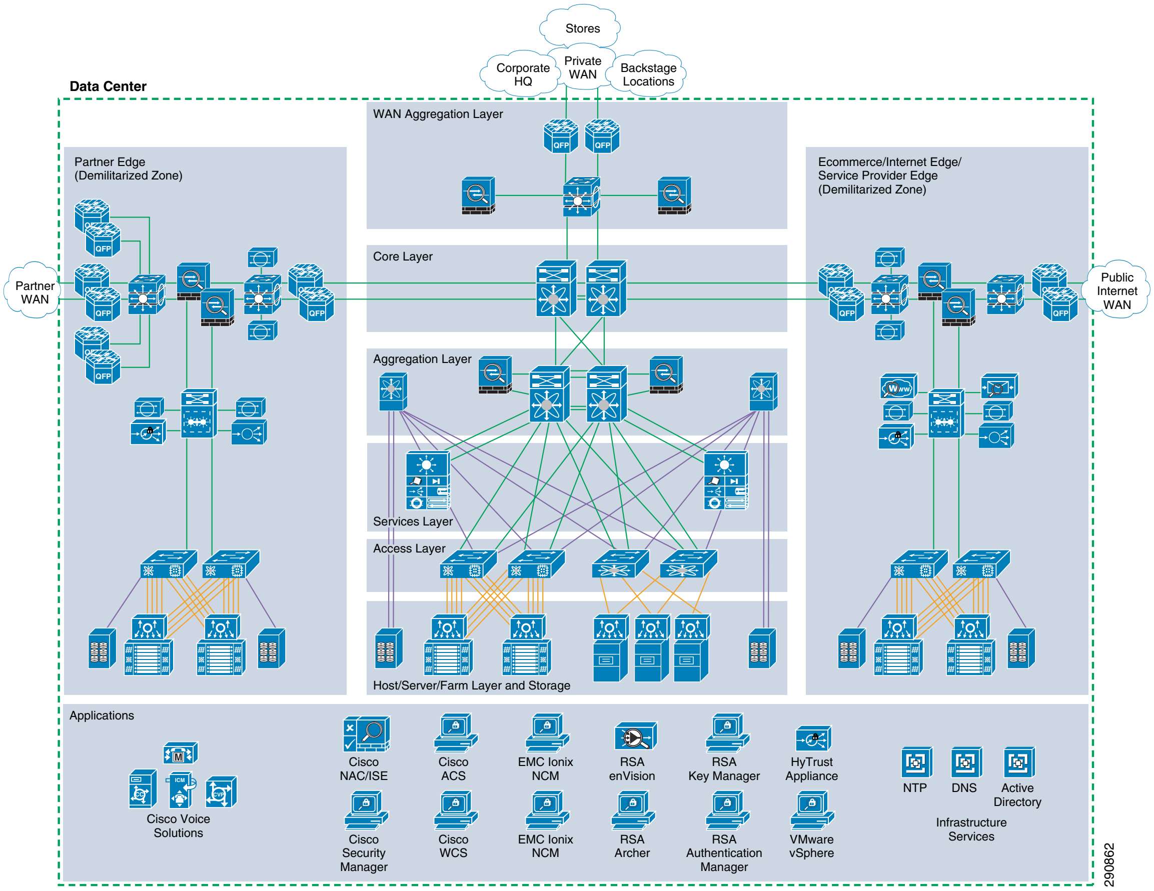
Components Selected

- Cisco 3945 Integrated Services Router (ISR)
- Cisco Catalyst 3560X and 4500 switches
- Cisco Aironet 3502e and 3502i Access Points
- Cisco 5508 Wireless Controller
- Cisco 4500 Video Surveillance Camera
- Cisco Physical Access Gateway

Data Center

The data center is where centralized data processing, data storage, and data communications take place (see Figure 4-13). The data center is also the place where management systems are deployed. The data center provides centralized control from an administrative perspective because it is typically where the tools that are used to monitor and enforce compliance are deployed.

Figure 4-13 Data Center Architecture



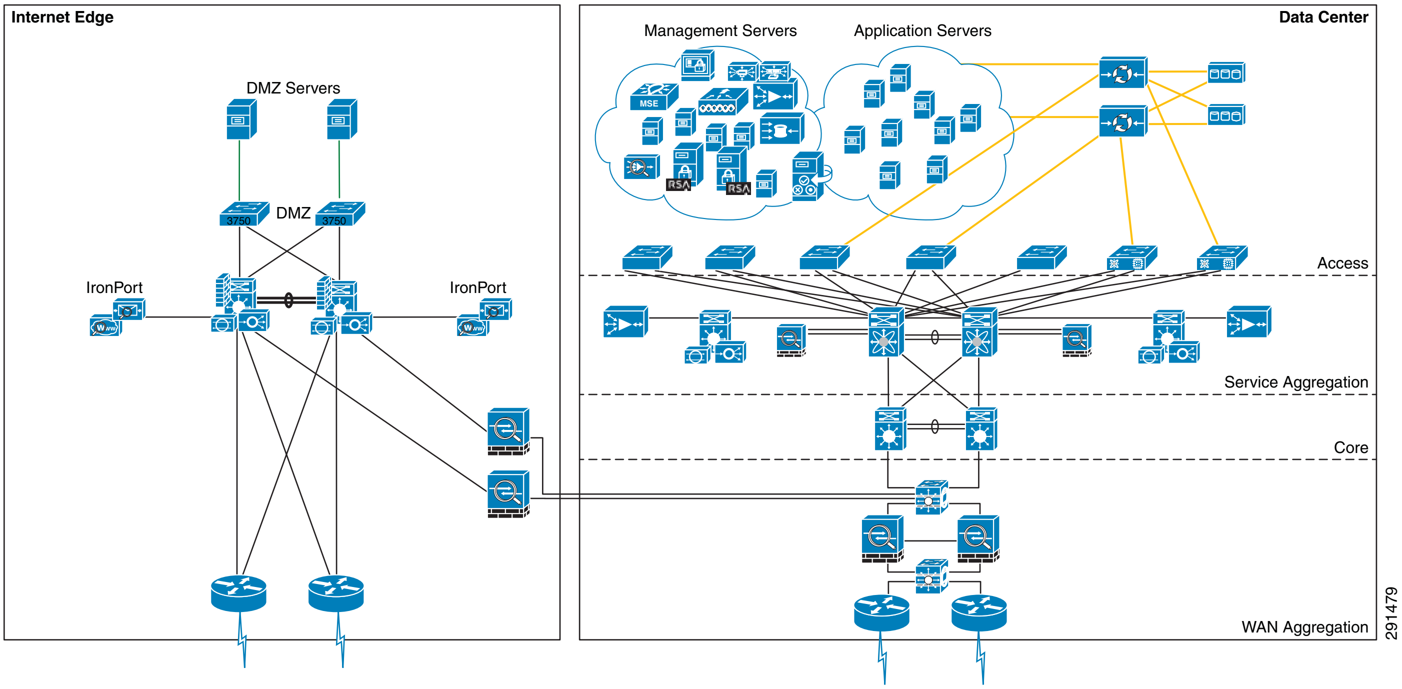
Design considerations are as follows:

- Centralized solution management supports all aspects of network, security, and systems management; and supports remote access from anywhere on the network.
- Standardized equipment and software images, deployed in a modular, layered approach, simplify configuration management and increase the systems availability.
- The highly available data center design permits highly resilient access from stores to core data and storage services.
- WAN aggregation alternatives allow flexible selection of service provider network offerings.
- The service aggregation design allows for a modular approach to adding new access layers and managing shared network services (for example, firewall, IPS, application networking, wireless management)

- Firewall, IPS, and application networking services are available at the service and aggregation layers of the data center.
- Scalability to accommodate shifting requirements in data center compute and storage requirements.
- WAN access speeds are typically the limiting factor between the store network systems and the WAN aggregation layer.
- It is typical for retailers to over-subscribe the WAN circuits between the stores and the WAN edge aggregation router. Over-subscription can cause inconsistent results and packet loss of payment card information in the event that more traffic enters the WAN circuit simultaneously.
- Backup network connections from store networks to the data center are recommended when payment card information is transported via the WAN.

Figure 4-14 shows the data center design.

Figure 4-14 Data Center Design



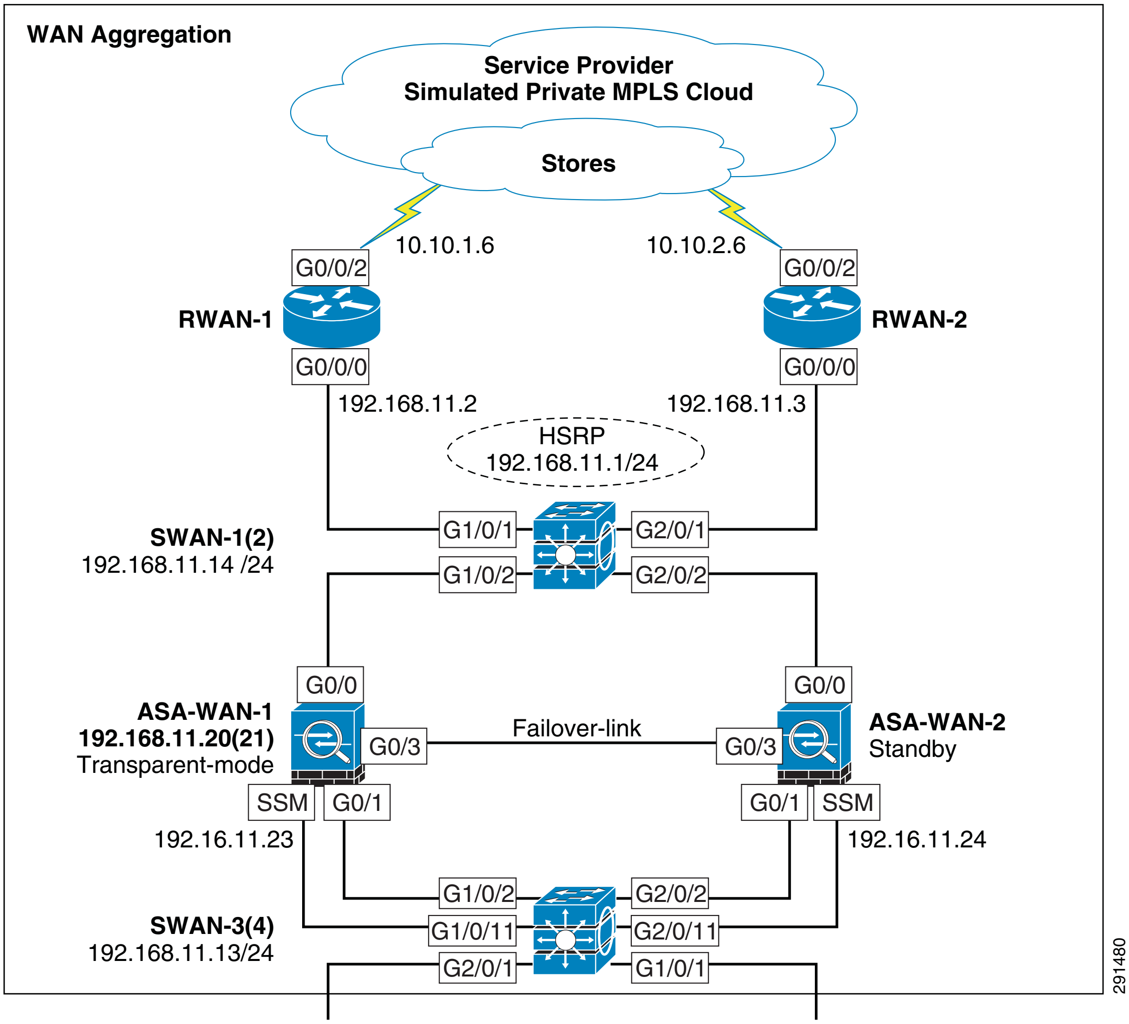
Data centers can house many types of functions and the term itself can encompass narrow and broad aspects. For the purposes of this guide, data centers include the following functions:

- WAN aggregation layer—Aggregates the store and backstage WAN connections to the core
- Core layer—Highly available, high-speed area that is the central point of connectivity to all data center areas
- Aggregation block—Aggregates the services of one area and connects that area to the core, including Vblock1 design
- Internet edge—Secure connectivity to the Internet

WAN Aggregation Layer Design

Figure 4-15 shows the WAN aggregation layer design.

Figure 4-15 WAN Aggregation Layer Design



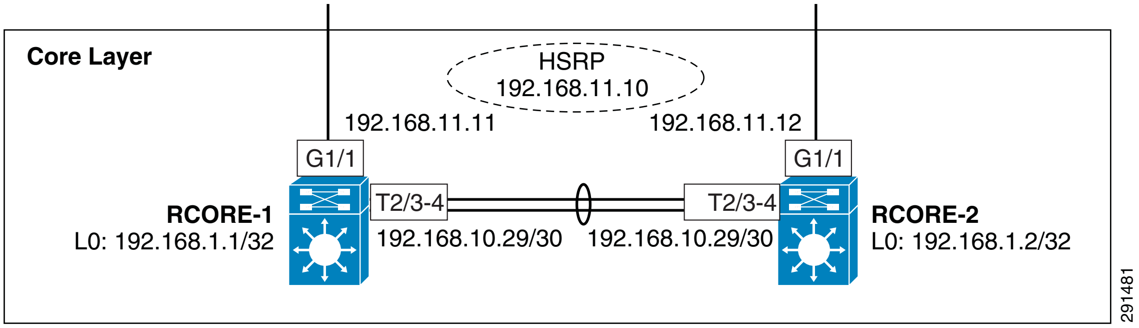
Components Selected

- Cisco ASR 1002-Fixed Router
- Cisco ASA 5540 Adaptive Security Appliance
- Cisco Catalyst 3750X Switch

Core Layer Design

Figure 4-16 shows the core layer design.

Figure 4-16 Core Layer Design



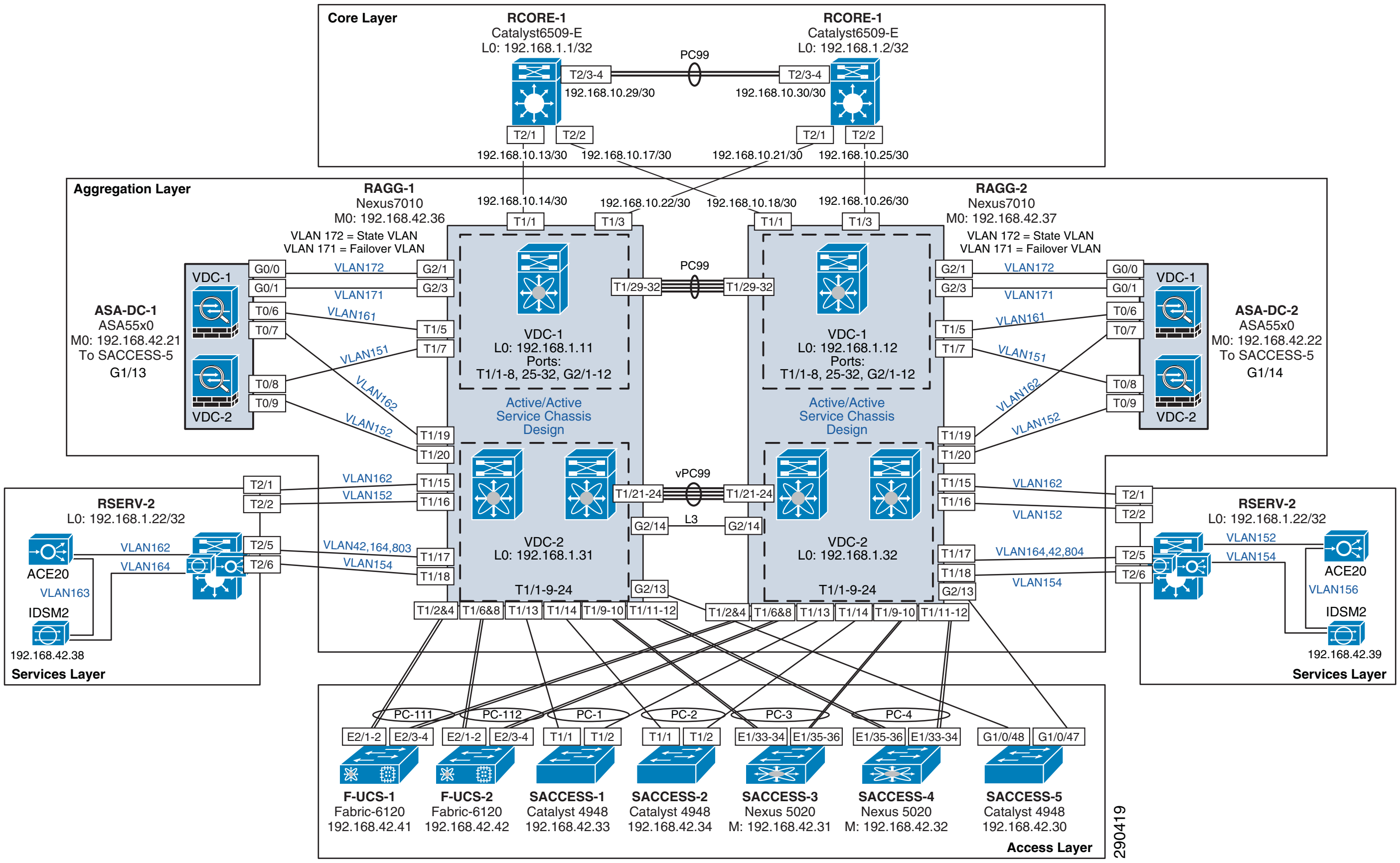
Components Selected

- Cisco Catalyst 6500-E Switch

Aggregation Block Design

Figure 4-17 shows the aggregation block design.

Figure 4-17 Aggregation Block Design



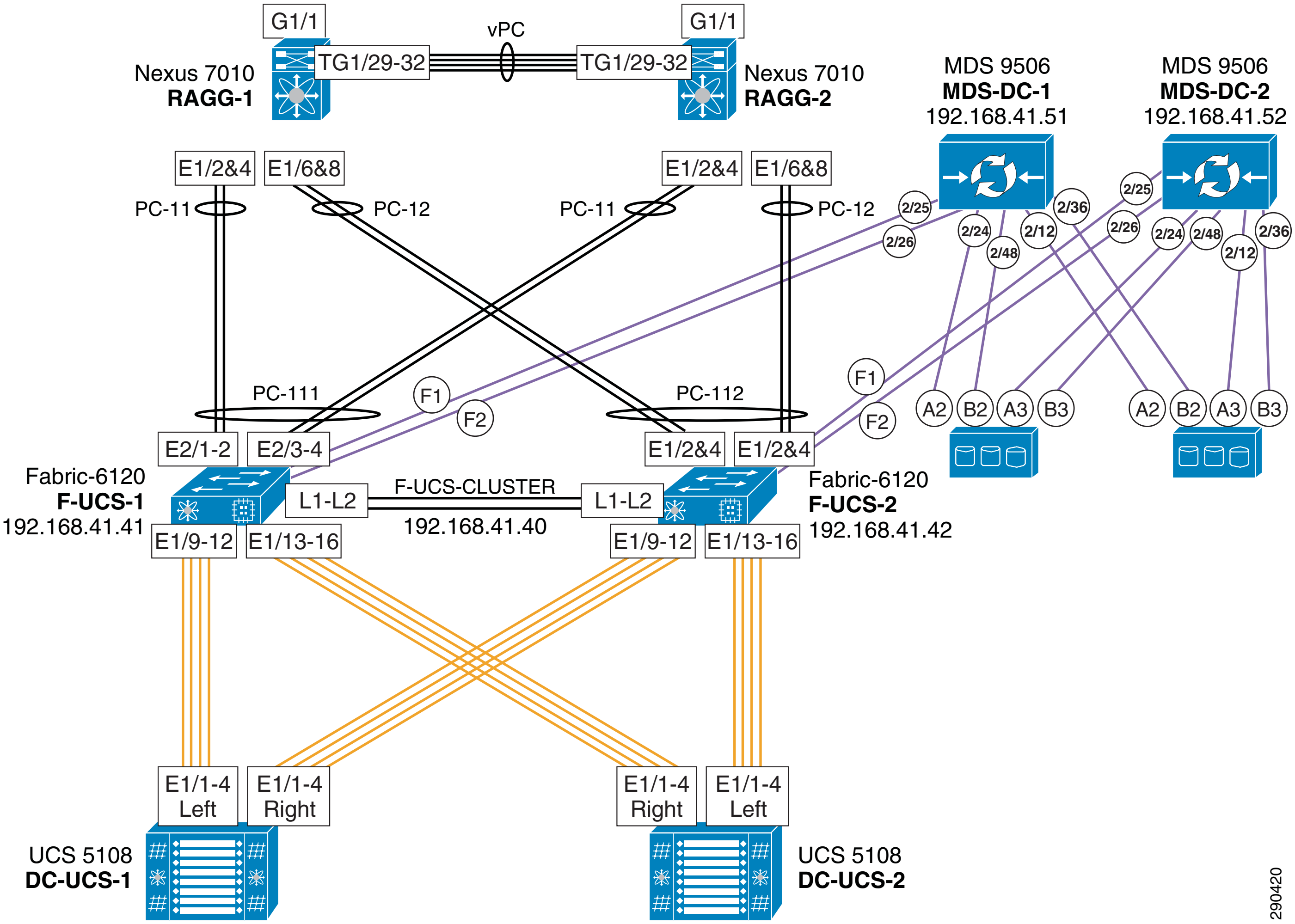
Components Selected

- Cisco ASA 5585-X Adaptive Security Appliance
- Cisco Nexus 7010 Switch
- Cisco Catalyst 6500-E Switch
    - Cisco ACE 20
    - Cisco IDSM-2
- Cisco Nexus 5020 Switch
- Cisco Catalyst 4948 Switch

Vblock Design

Figure 4-18 shows the Vblock design.

Figure 4-18 Vblock Design



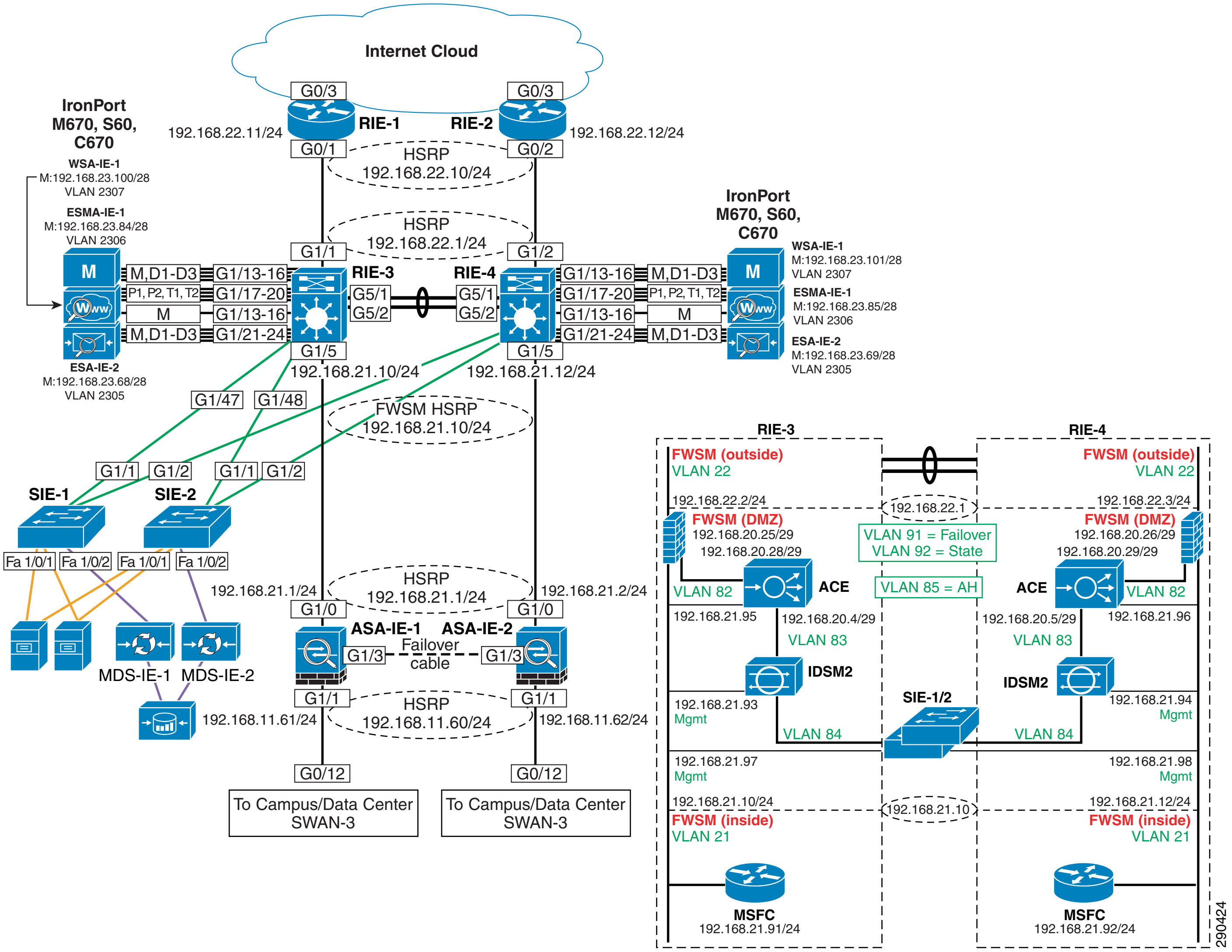
Components Selected

- Cisco UCS 5108 Blade Server Chassis
  - Cisco UCS B200 Blade Server
- Cisco UCS 6120 Fabric Interconnect
- Cisco MDS 9506 Multilayer Director
- EMC CLARiion CX4 Model 240

Internet Edge Design

Figure 4-19 shows the Internet edge network design.

Figure 4-19 Internet Edge Network Design



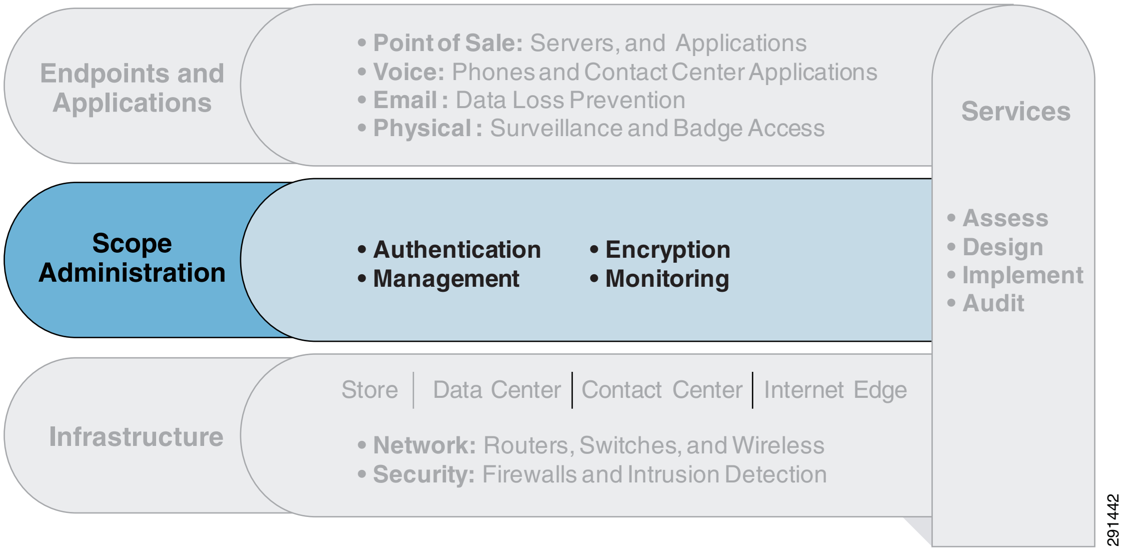
Components Selected

- Cisco 7200 Series Router
- Cisco Catalyst 6500-E Switch
  - Cisco ACE 20
  - Cisco IDSM-2
- Cisco Catalyst 3750X Switch
- Cisco MDS 9204i Switch
- Cisco IronPort C670

Scope Administration

The scope administration layer of the solution framework addresses the components such as authentication, encryption, management, and monitoring, as shown in Figure 4-20.

Figure 4-20 Scope Administration Layer of the Solution Framework


Endpoints and Applications
• Point of Sale: Servers, and Applications
• Voice: Phones and Contact Center Applications
• Email : Data Loss Prevention
• Physical : Surveillance and Badge Access
Services
Scope Administration
• Authentication
• Encryption
• Management
• Monitoring
• Assess
• Design
• Implement
• Audit
Infrastructure
Store
Data Center
Contact Center
Internet Edge
• Network: Routers, Switches, and Wireless
• Security: Firewalls and Intrusion Detection
291442

Authentication

Components Selected

- Cisco Secure Access Control Server (ACS)
- Cisco Identity Services Engine (ISE)
- RSA Authentication Manager
- Windows Active Directory

Encryption

Components Selected

- Cisco Security Manager
- Cisco Key Manager
- RSA Data Protection Manager

Management

Components Selected

- EMC Ionix Network Configuration Manager (NCM)
- Cisco Security Manager
- Cisco Wireless Control Server Manager
- EMC Unified Infrastructure Manager
- VMware vSphere vCenter
- Cisco Video Surveillance Manager
- Cisco Physical Access Manager
- RSA Archer

Monitoring

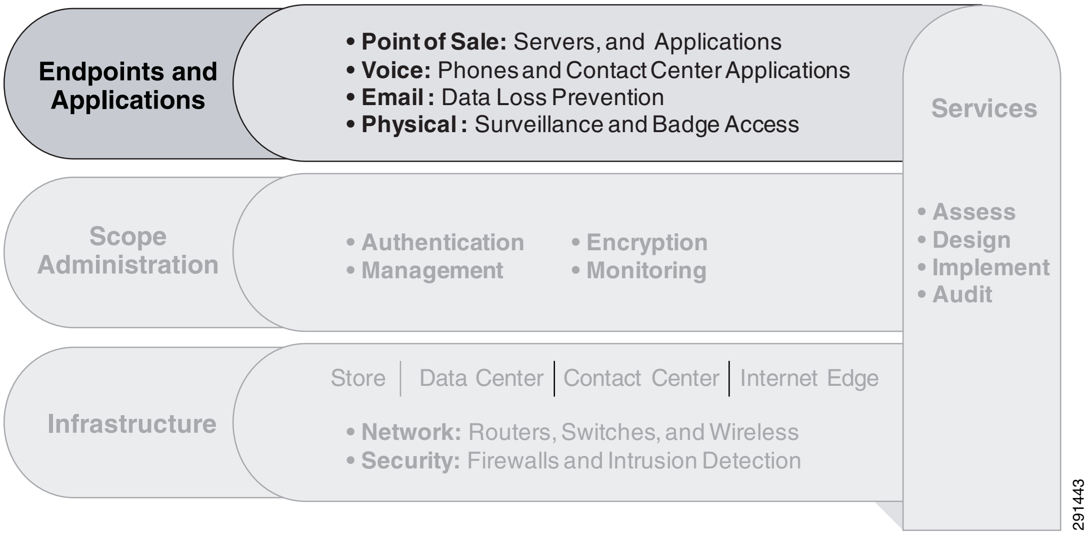
Components Selected

- RSA enVision
- HyTrust
- EMC Ionix Network Configuration Manager (NCM)

Endpoints and Applications

The endpoints and applications layer of the solution framework addresses the components such as voice, e-mail, and physical security, as shown in Figure 4-21.

Figure 4-21 Endpoints and Applications Layer of the PCI Solution Framework


Endpoints and Applications
• Point of Sale: Servers, and Applications
• Voice: Phones and Contact Center Applications
• Email : Data Loss Prevention
• Physical : Surveillance and Badge Access
Services
Scope Administration
• Authentication
• Management
• Encryption
• Monitoring
• Assess
• Design
• Implement
• Audit
Infrastructure
Store
Data Center
Contact Center
Internet Edge
• Network: Routers, Switches, and Wireless
• Security: Firewalls and Intrusion Detection
291443

Voice

Components Selected

- Cisco Unified Communications Manager
- Cisco IP Phones (9971, 7975)
- Cisco Survivable Remote Site Telephony (SRST)

E-mail

Components Selected

- Cisco IronPort Email Security Appliance with Data Loss Prevention
- Microsoft Exchange Server 2008

Physical

Components Selected

- Cisco Physical Access Gateway
- Cisco Video Surveillance Cameras (2421, 2500, 4500)

Note For a complete Bill of Materials, see Appendix A, “Bill Of Material.” For assessment of components selected for PCI compliance, see Chapter 5, “Component Assessment.” For complete running configurations of components, see Appendix E, “Detailed Full Running Configurations.”

CHAPTER 5

Component Assessment

This chapter discusses the function of each component and how it helps to address PCI DSS 2.0 compliance requirements. Each component was assessed by Verizon Business, and the full reference architecture report is available in Appendix B, "Verizon Business Reference Architecture Report—Cisco PCI Solution for Retail."

This assessment took place at a specific point in time using currently available versions of products and software.

Component Section Overview

Each component section includes the following:

- Description
- PCI assessment summary
- Primary PCI function
- Capability assessment
- Design considerations
- PCI assessment detail

PCI Assessment Summary

For each component, the PCI Assessment Summary table (see Table 5-1) lists each of the PCI sub-requirements that were passed, required compensating controls, or failed.

Table 5-1 PCI Assessment Summary Example

Models Assessed	
Cisco Catalyst Switch	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3

Table 5-1 PCI Assessment Summary Example (continued)

PCI 6	6.1
PCI 7	7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Capability Assessment

Each component requires specific capabilities to be deployable in a compliant environment. Customers and vendors alike have complained that it is difficult to understand what capabilities are required when developing or purchasing equipment for the purpose of compliance. Therefore, Cisco has developed a simplified approach to clarify the scales that are relevant. Sub-requirements have been grouped for ease of assessment, as shown in Table 5-1.

Table 5-2 Capability Assessment Example

Cisco Component	
PRIMARY FUNCTION	**Requirement 9 (9.1.2)**
[Description of primary PCI function]	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

The PCI DSS 2.0 security standard is written from the perspective of helping a merchant become compliant. It is not grouped in a clear manner for the evaluation of hardware or software. The following grouping of sub-requirements is an extrapolation of the standard to simplify the assessment of hardware and software:

- *Secure services* comprises sub-requirements that affect the secure administration and hardening of the component, and include the following:
  - Disable any unnecessary services—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers*. (Sub-requirements 2.2.2, 2.2.4)
  - Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)
  - Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)
- *Authentication* comprises sub-requirements that affect the identity of personnel accessing systems in the cardholder data environment, including the following:
  - Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed*. (Sub-requirement 7.1, 7.2)
  - Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data. Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
- *Logs* comprises sub-requirements that affect the forensic analysis capabilities of the cardholder data environment, including the following:
  - Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)
  - The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources*. (Sub-requirements 10.4.2, 10.4.3)

Table 5-3 explains the color-codes icons used in the tables.

Table 5-3 Color-Coded Icon Definitions

Icon	Description
🟢	The component has the native capability to satisfy the requirement.
◉	The component has the capability to use other components to satisfy the requirement.
▼	The component requires compensating controls to satisfy the requirement.
⊗	The component has no capability to satisfy the requirement.

Design Considerations

This section provides compliance principles as well as best practices for each technology deployed within a retail business environment.

PCI Assessment Detail

This section includes the following:

- PCI sub-requirements satisfied by solution component—Lists which PCI sub-requirements were successfully audited and validated by the respective technology. Each sub-requirement includes a configuration example or reference of how the sub-requirement was met. This result is directly correlated to the implementation built in the Cisco lab and presented in Chapter 4, "Implementing and Configuring the Solution."
- PCI sub-requirements that require compensating controls—Lists which PCI sub-requirements needed additional compensating controls to successfully pass the PCI audit. Examples include additional configurations, products, or policies to meet compliance requirements.
- PCI sub-requirements that failed—Lists which PCI sub-requirements could not be satisfied.

Endpoints and Applications

The endpoints and applications layer of the solution framework addresses the components such as voice, e-mail, and physical security.

Voice

Cisco Unified Communications Manager and IP Phones

The Cisco Unified Communication Manager is a suite of voice applications, signaling control, and utilities that provide IP communications capabilities using devices such as the IP phones. It is configured as an appliance that is easy to deploy, flexible to manage, and allows robust security.

Table 5-4 PCI Assessment Summary—Cisco Unified Communications Manager

Models Assessed	
Cisco Unified Communication Manager 8.5.1	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 9	9.1.2
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5

Table 5-4 PCI Assessment Summary—Cisco Unified Communications Manager (continued)

PCI Sub-Requirements Requiring Compensating Controls
No compensating controls were required to satisfy any sub-requirements.
PCI Sub-Requirements Failed
No sub-requirements were failed.

Primary PCI Function

The primary PCI function of Cisco Unified Communications Manager is to securely manage IP phones and communications flows, as well as securing publicly accessible network jacks (9.1.2).

Table 5-4 lists the component assessment details for Cisco Unified Communications Manager.

Table 5-5 Component Capability Assessment—Cisco Unified Communications Manager

Cisco Unified Communications Manager	
PRIMARY FUNCTION	**Requirement 9 (9.1.2)**
Securely manage IP phones and communication flows.	
CAPABILITY	ASSESSMENT
Secure Services	
Disabled any unnecessary services—*“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

The design features for improving security for the Cisco Unified Communications Manager appliance include:

- Deployment as a clustered redundancy model that includes a publisher server and several subscriber servers
- Downloading and installing security patches when vulnerabilities are announced by the Cisco Product Security Incident Response Team (PSIRT)
- Implementing Transport Layer Security (TLS) messaging for secure signaling and Secure RTP (SRTP) for encrypted media throughout the enterprise
- Enabling device authentication and communication encryption using X.509 certificates that are signed by the Certificate Authority Proxy Function (CAPF) feature on the server

Best practices for Cisco Unified Communications Manager phone security are as follows:

- The Gratuitous ARP setting on the Cisco Unified IP Phones should be disabled.
- Disabling the web access setting prevents the phone from opening the HTTP port 80; this blocks access to the phone’s internal web pages.
- Disabling the PC Voice VLAN access setting in the phone configuration window prevents the devices connected to the PC port from using the voice VLAN functionality.
- Disabling the Setting Access option in the phone configuration window prevents users from viewing and changing the phone options, including the Network Configuration options, directly on the phone.
- Cisco Unified IP Phones can be configured for authentication and encryption by installing a CTL file on the phones that includes security tokens, trusted server and firewall information, and CAPF.

For more information on securing Unified Communications, see the *Cisco Unified Communications System 8.x SRND* at the following URL:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/security.html

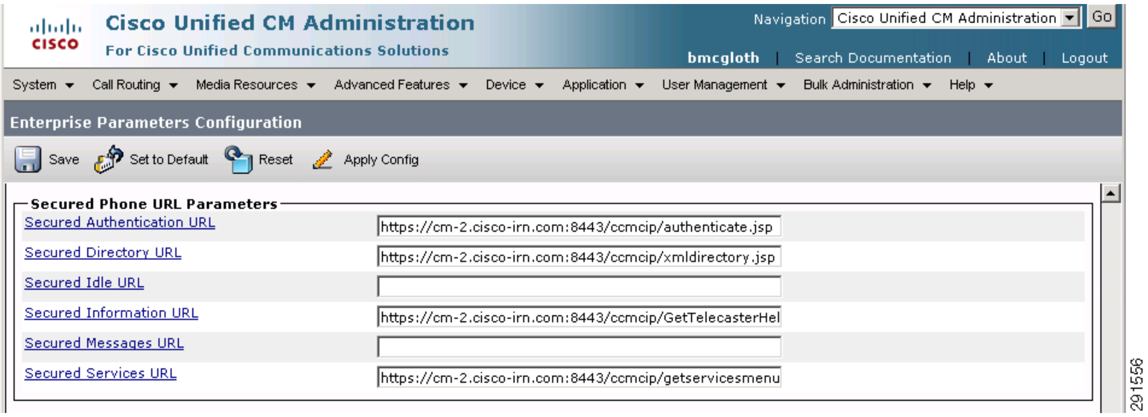
PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The Cisco Unified Communication Manager appliance operating system includes only the components needed to run the application. Root access to the OS is disabled and this prevents any unwanted services from being implemented. Telnet and HTTP access to the server administration is disabled. The communication between phones and server over HTTP can be secured using SSL. (See Figure 5-1.)

Figure 5-1 Enterprise Parameters Configuration



Secured Phone URL Parameters

Secured Authentication URL	https://cm-2.cisco-irn.com:8443/ccmcip/authenticate.jsp
Secured Directory URL	https://cm-2.cisco-irn.com:8443/ccmcip/xmldirectory.jsp
Secured Idle URL	
Secured Information URL	https://cm-2.cisco-irn.com:8443/ccmcip/GetTelecasterHel
Secured Messages URL	
Secured Services URL	https://cm-2.cisco-irn.com:8443/ccmcip/getservicesmenu

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco Unified Communication Manager appliance does not allow changes to the operating system, or to the database or installation of unsupported hardware or of unsupported third-party software.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The Cisco Unified Communication Manager uses SSL for web-based administrative and user access and uses SSH for remote terminal access.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in the Cisco Unified Communication Manager appliance. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise through a web browser or CLI.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

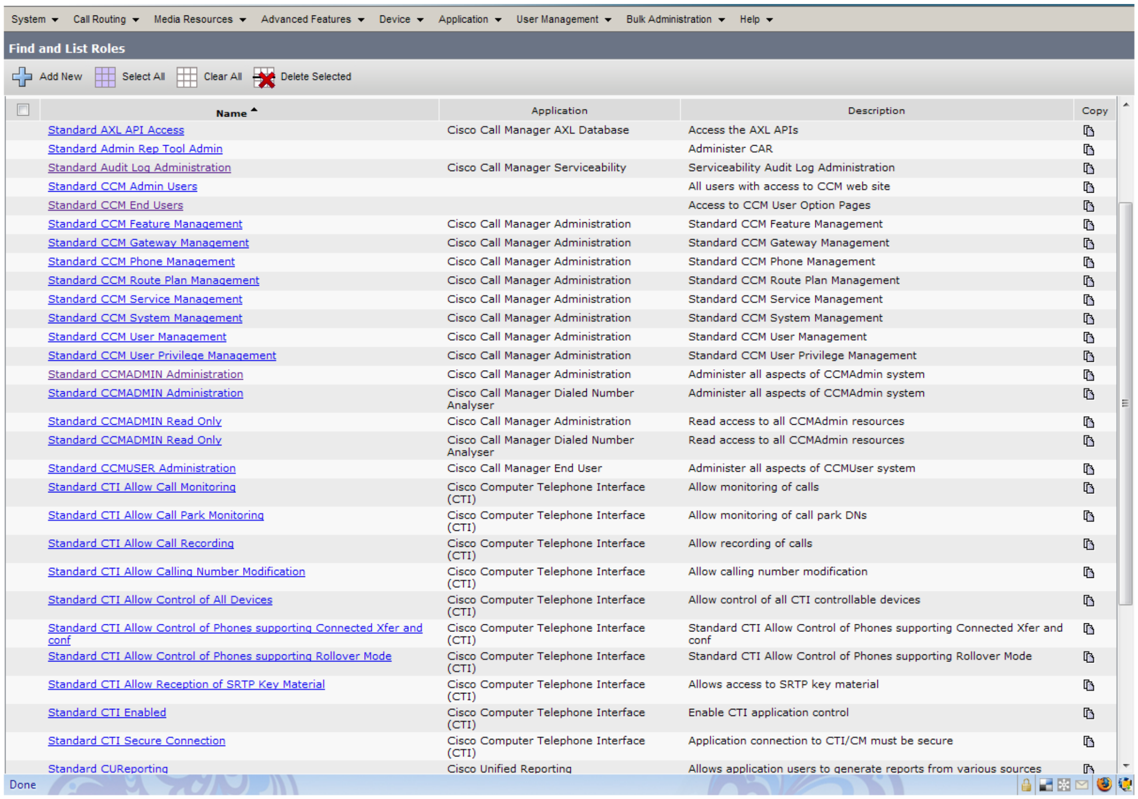
The relevant sub-requirements of Requirement 7 were met using the Cisco Unified Communication Manager's internal database. Cisco Unified Communication Manager also supports linking to a centralized user database such as Active Directory using LDAP. Within Cisco Unified Communication Manager, individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*

- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

  The Cisco Unified Communication Manager uses various role definitions for permitting access to various application components on the server. (See Figure 5-2.)

Figure 5-2 Find and List Roles

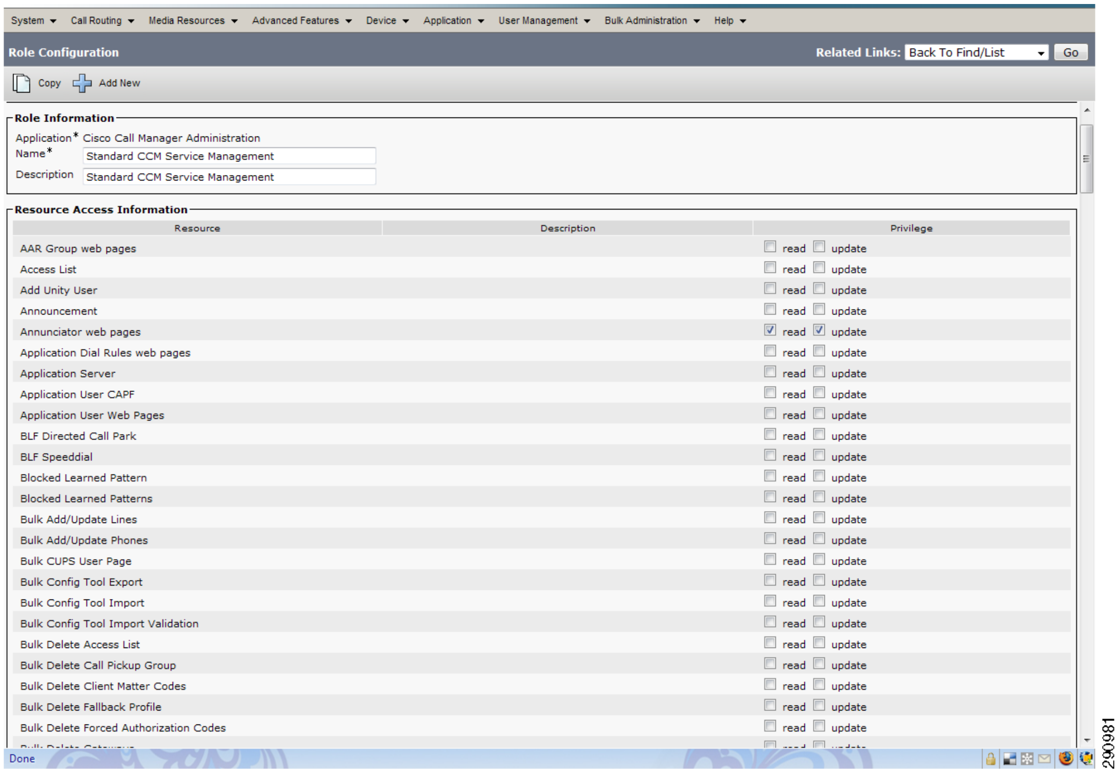


□	Name	Application	Description	Copy
	Standard AXL API Access	Cisco Call Manager AXL Database	Access the AXL APIs	⎘
	Standard Admin Rep Tool Admin		Administer CAR	⎘
	Standard Audit Log Administration	Cisco Call Manager Serviceability	Serviceability Audit Log Administration	⎘
	Standard CCM Admin Users		All users with access to CCM web site	⎘
	Standard CCM End Users		Access to CCM User Option Pages	⎘
	Standard CCM Feature Management	Cisco Call Manager Administration	Standard CCM Feature Management	⎘
	Standard CCM Gateway Management	Cisco Call Manager Administration	Standard CCM Gateway Management	⎘
	Standard CCM Phone Management	Cisco Call Manager Administration	Standard CCM Phone Management	⎘
	Standard CCM Route Plan Management	Cisco Call Manager Administration	Standard CCM Route Plan Management	⎘
	Standard CCM Service Management	Cisco Call Manager Administration	Standard CCM Service Management	⎘
	Standard CCM System Management	Cisco Call Manager Administration	Standard CCM System Management	⎘
	Standard CCM User Management	Cisco Call Manager Administration	Standard CCM User Management	⎘
	Standard CCM User Privilege Management	Cisco Call Manager Administration	Standard CCM User Privilege Management	⎘
	Standard CCMADMIN Administration	Cisco Call Manager Administration	Administer all aspects of CCMAdmin system	⎘
	Standard CCMADMIN Administration	Cisco Call Manager Dialed Number Analyser	Administer all aspects of CCMAdmin system	⎘
	Standard CCMADMIN Read Only	Cisco Call Manager Administration	Read access to all CCMAdmin resources	⎘
	Standard CCMADMIN Read Only	Cisco Call Manager Dialed Number Analyser	Read access to all CCMAdmin resources	⎘
	Standard CCMUSER Administration	Cisco Call Manager End User	Administer all aspects of CCMUser system	⎘
	Standard CTI Allow Call Monitoring	Cisco Computer Telephone Interface (CTI)	Allow monitoring of calls	⎘
	Standard CTI Allow Call Park Monitoring	Cisco Computer Telephone Interface (CTI)	Allow monitoring of call park DNs	⎘
	Standard CTI Allow Call Recording	Cisco Computer Telephone Interface (CTI)	Allow recording of calls	⎘
	Standard CTI Allow Calling Number Modification	Cisco Computer Telephone Interface (CTI)	Allow calling number modification	⎘
	Standard CTI Allow Control of All Devices	Cisco Computer Telephone Interface (CTI)	Allow control of all CTI controllable devices	⎘
	Standard CTI Allow Control of Phones supporting Connected Xfer and conf	Cisco Computer Telephone Interface (CTI)	Standard CTI Allow Control of Phones supporting Connected Xfer and conf	⎘
	Standard CTI Allow Control of Phones supporting Rollover Mode	Cisco Computer Telephone Interface (CTI)	Standard CTI Allow Control of Phones supporting Rollover Mode	⎘
	Standard CTI Allow Reception of SRTP Key Material	Cisco Computer Telephone Interface (CTI)	Allows access to SRTP key material	⎘
	Standard CTI Enabled	Cisco Computer Telephone Interface (CTI)	Enable CTI application control	⎘
	Standard CTI Secure Connection	Cisco Computer Telephone Interface (CTI)	Application connection to CTI/CM must be secure	⎘
	Standard CUReporting	Cisco Unified Reporting	Allows application users to generate reports from various sources	⎘

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

The role configuration menu in the Cisco Unified Communication Manager server allows specifying the assignment of privileges based on the role description. No systems access is permitted without an account. (See Figure 5-3.)

Figure 5-3 Role Configuration



Role Configuration

Role Information

Application* Cisco Call Manager Administration
Name* Standard CCM Service Management
Description Standard CCM Service Management

Resource Access Information

Resource	Description	Privilege
AAR Group web pages		□ read □ update
Access List		□ read □ update
Add Unity User		□ read □ update
Announcement		□ read □ update
Annunciator web pages		☑ read ☑ update
Application Dial Rules web pages		□ read □ update
Application Server		□ read □ update
Application User CAPF		□ read □ update
Application User Web Pages		□ read □ update
BLF Directed Call Park		□ read □ update
BLF Speeddial		□ read □ update
Blocked Learned Pattern		□ read □ update
Blocked Learned Patterns		□ read □ update
Bulk Add/Update Lines		□ read □ update
Bulk Add/Update Phones		□ read □ update
Bulk CUPS User Page		□ read □ update
Bulk Config Tool Export		□ read □ update
Bulk Config Tool Import		□ read □ update
Bulk Config Tool Import Validation		□ read □ update
Bulk Delete Access List		□ read □ update
Bulk Delete Call Pickup Group		□ read □ update
Bulk Delete Client Matter Codes		□ read □ update
Bulk Delete Fallback Profile		□ read □ update
Bulk Delete Forced Authorization Codes		□ read □ update

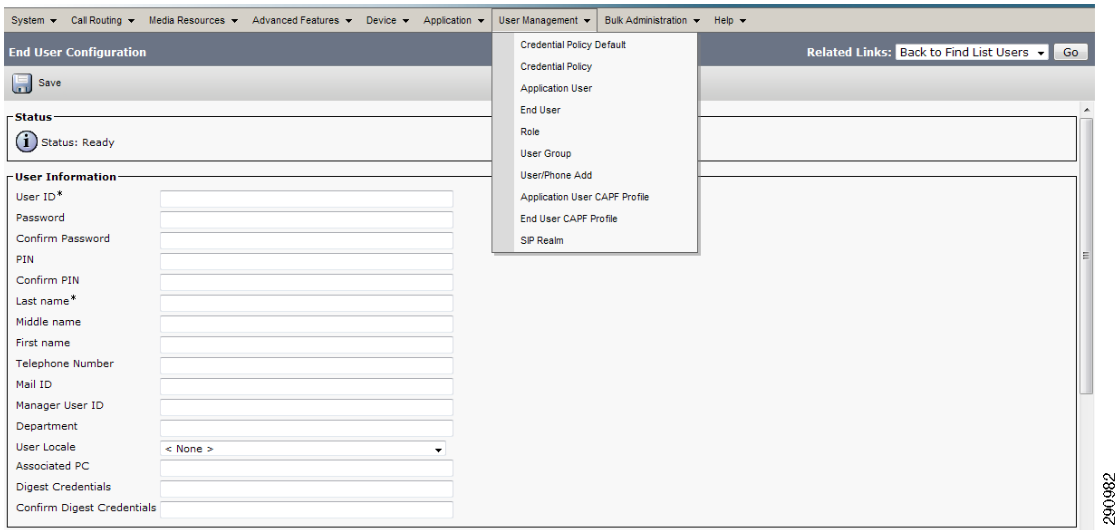
Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database, as shown below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Sub-requirements 8.1, 8.2, and 8.4 are met by configuring user IDs and passwords in the User Management section of the Cisco Unified Communication manager web interface, as shown in Figure 5-4.

Figure 5-4 End User Configuration



End User Configuration

Status

Status: Ready

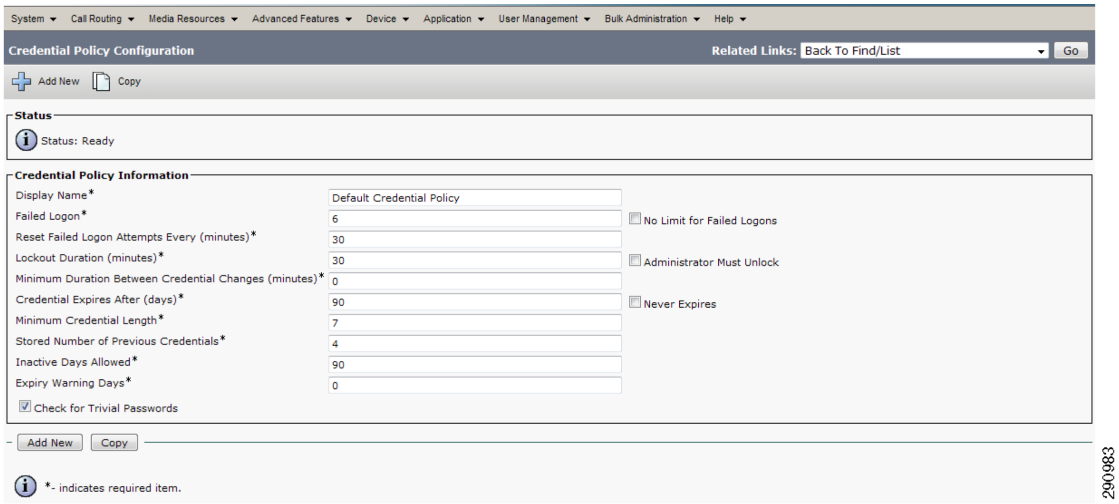
User Information

User ID*
Password
Confirm Password
PIN
Confirm PIN
Last name*
Middle name
First name
Telephone Number
Mail ID
Manager User ID
Department
User Locale < None >
Associated PC
Digest Credentials
Confirm Digest Credentials

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Sub-requirements 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, and 8.5.14 are met by configuring a credential policy for user management and applying that policy to a designated group. Figure 5-5 shows a modified default credential policy.

Figure 5-5 User Credential Policy Configuration


System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
Credential Policy Configuration
Related Links: Back To Find/List ▾ Go
Add New
Copy
Status
Add New
Copy
290983

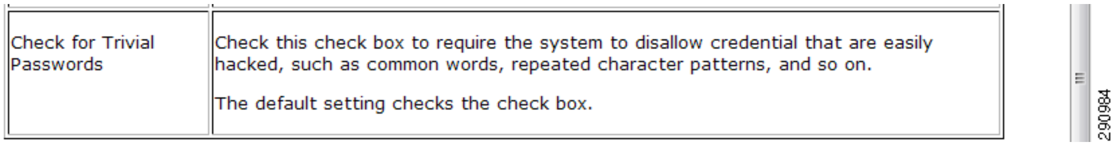
Status: Ready

Credential Policy Information

Display Name*	Default Credential Policy	
Failed Logon*	6	□ No Limit for Failed Logons
Reset Failed Logon Attempts Every (minutes)*	30	
Lockout Duration (minutes)*	30	□ Administrator Must Unlock
Minimum Duration Between Credential Changes (minutes)*	0	
Credential Expires After (days)*	90	□ Never Expires
Minimum Credential Length*	7	
Stored Number of Previous Credentials*	4	
Inactive Days Allowed*	90	
Expiry Warning Days*	0	

☑ Check for Trivial Passwords

*- indicates required item.



Check for Trivial Passwords	Check this check box to require the system to disallow credential that are easily hacked, such as common words, repeated character patterns, and so on. The default setting checks the check box.

The system provides trivial credential checks to disallow credentials that are easily hacked. You enable trivial credential checks by checking the Check for Trivial Passwords check box in the Credential Policy Configuration window.

Passwords can contain any alphanumeric ASCII character and all ASCII special characters. A non-trivial password meets the following criteria:

- Must contain three of the four allowable characteristics: uppercase character, lowercase character, number, and symbol.
- Must not use a character or number more than three times consecutively.
- Must not repeat or include the alias, username, or extension.
- Cannot consist of consecutive characters or numbers (for example, passwords such as 654321 or ABCDEFG)

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

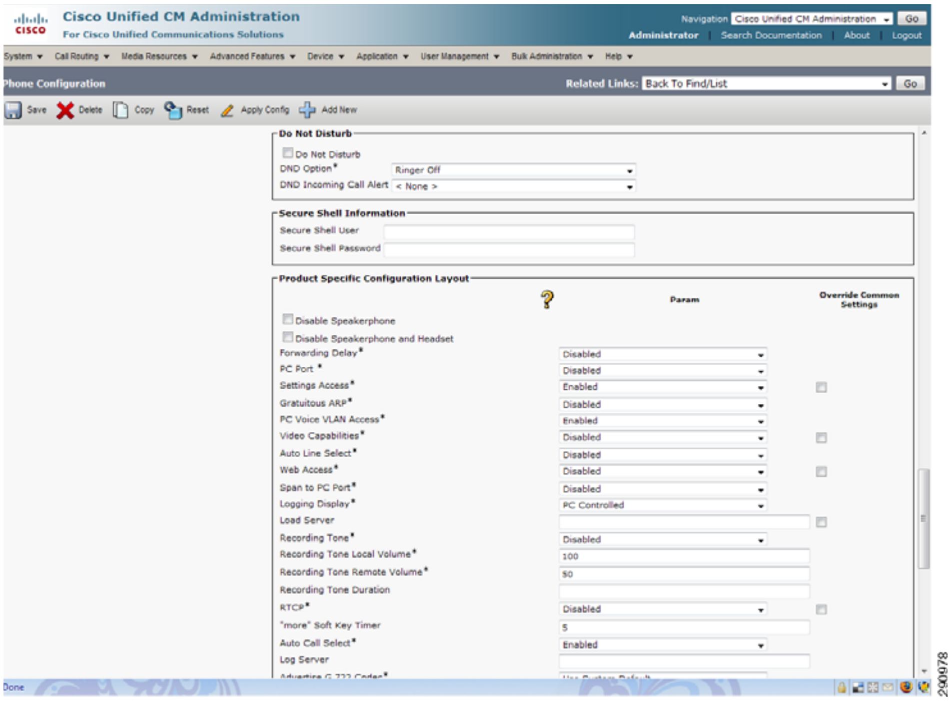
  Sub-requirement 8.5.15 is part of the default system behavior. The system locks the user's session if the session has been idle for fifteen minutes, requiring the user to login again.

Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.2**—*Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.*

  This requirement is met by disabling the PC port setting in the phone configuration window for ports that are not in use, as shown in Figure 5-6.

Figure 5-6 Phone Configuration


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
Administrator | Search Documentation | About | Logout
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
Related Links: Back To Find/List Go
Save Delete Copy Reset Apply Config Add New
Done
290978

Phone Configuration

Do Not Disturb

□ Do Not Disturb

DND Option* Ringer Off

DND Incoming Call Alert < None >

Secure Shell Information

Secure Shell User

Secure Shell Password

Product Specific Configuration Layout

□ Disable Speakerphone

□ Disable Speakerphone and Headset

	Param	Override Common Settings
Forwarding Delay*	Disabled	
PC Port *	Disabled	
Settings Access*	Enabled	□
Gratuitous ARP*	Disabled	
PC Voice VLAN Access*	Enabled	
Video Capabilities*	Disabled	□
Auto Line Select*	Disabled	
Web Access*	Disabled	□
Span to PC Port*	Disabled	
Logging Display*	PC Controlled	
Load Server		□
Recording Tone*	Disabled	
Recording Tone Local Volume*	100	
Recording Tone Remote Volume*	50	
Recording Tone Duration		
RTCP*	Disabled	□
"more" Soft Key Timer	5	
Auto Call Select*	Enabled	
Log Server		
Advertise G.722 Codec*	Use System Default	

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco Unified Communications Manager is able to track and monitor all administrative user access and events.

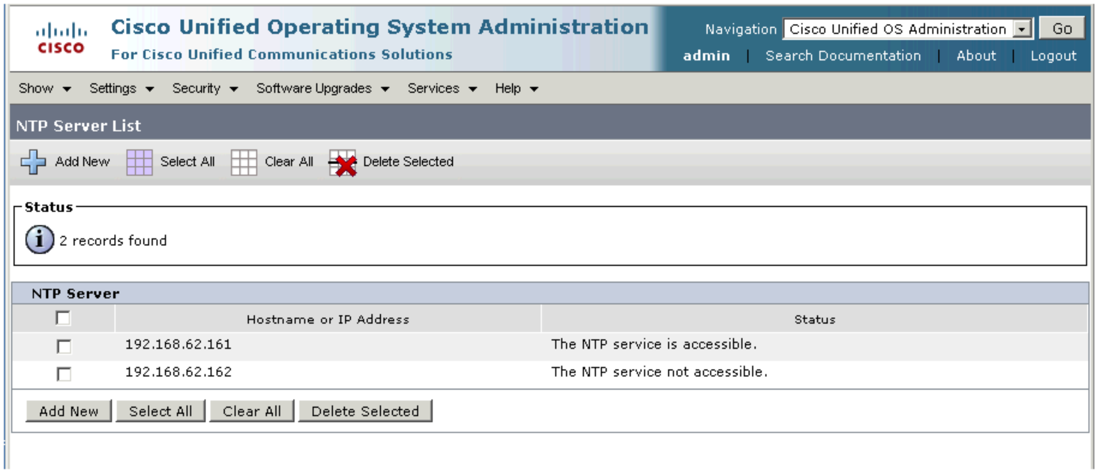
- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Unified Communication manager uses Network Time Protocol (NTP) to update and synchronize local clock facilities to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. This requirement is met by configuring the NTP server, as shown in Figure 5-7.

Figure 5-7 NTP Server List



2 records found

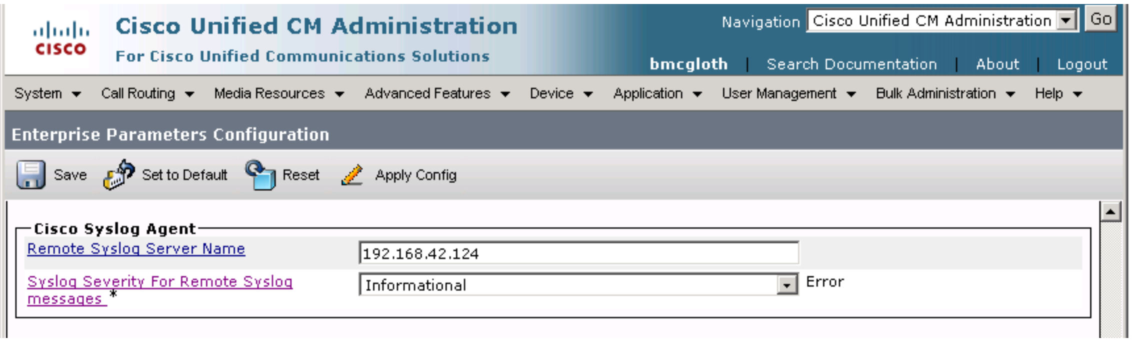
□	Hostname or IP Address	Status
□	192.168.62.161	The NTP service is accessible.
□	192.168.62.162	The NTP service not accessible.

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  The Cisco Unified Communication Manager can be configured to send the logs to an external syslog server where it cannot be altered by the appliance users. Figure 5-8 and Figure 5-9 show the configurations necessary for log forwarding.

Figure 5-8 Enterprise Parameters Configuration


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
bmcgloth | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Save Set to Default Reset Apply Config
291558

Enterprise Parameters Configuration

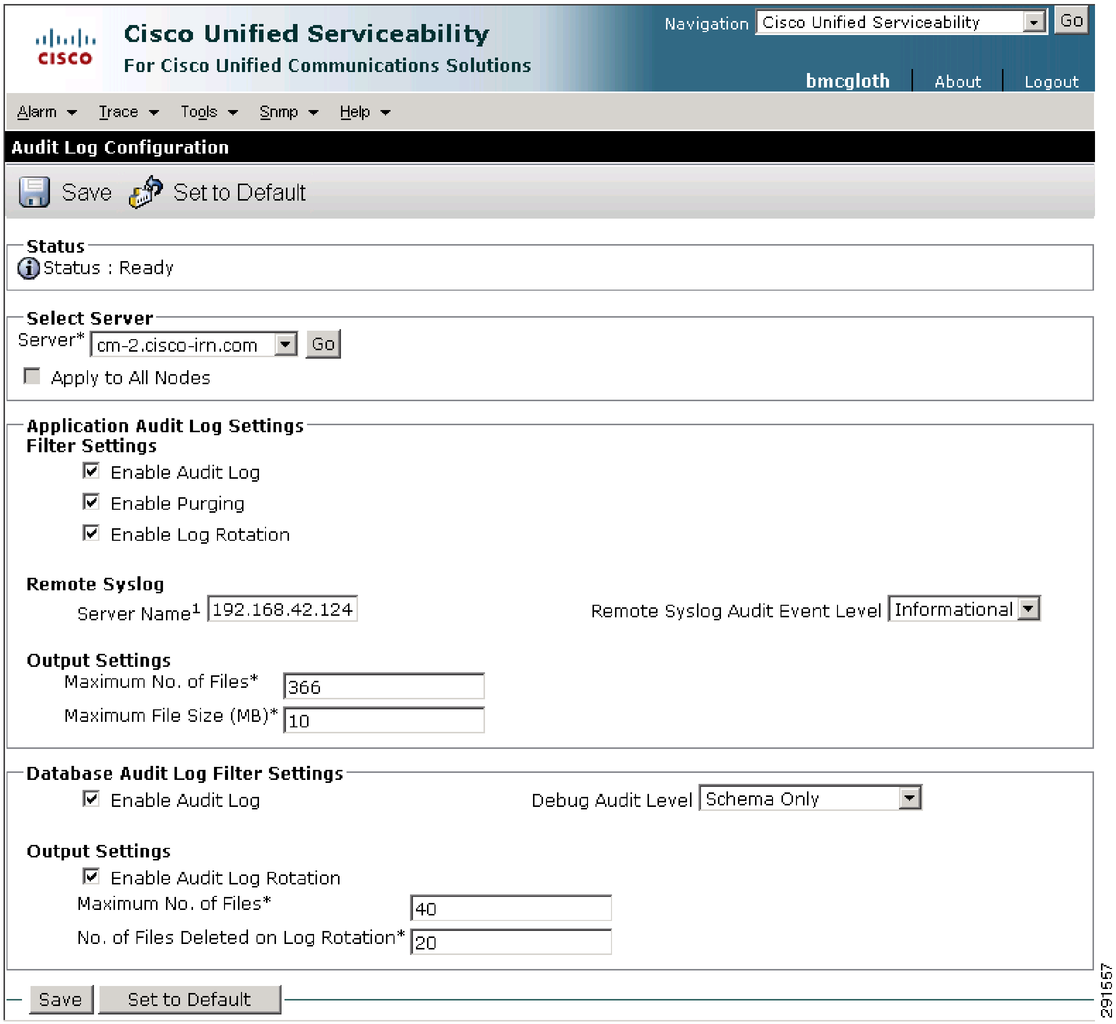
Cisco Syslog Agent

Remote Syslog Server Name: 192.168.42.124

Syslog Severity For Remote Syslog messages *: Informational — Error

Figure 5-9 shows the necessary configuration under Cisco Unified Serviceability.

Figure 5-9 Audit Log Configuration


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation Cisco Unified Serviceability Go
bmcgloth | About | Logout
Alarm Trace Tools Snmp Help
Save Set to Default
Go
Save Set to Default
291567

Audit Log Configuration

Status

Status : Ready

Select Server

Server*: cm-2.cisco-irn.com

□ Apply to All Nodes

Application Audit Log Settings

Filter Settings

☑ Enable Audit Log

☑ Enable Purging

☑ Enable Log Rotation

Remote Syslog

Server Name¹: 192.168.42.124 Remote Syslog Audit Event Level: Informational

Output Settings

Maximum No. of Files*: 366

Maximum File Size (MB)*: 10

Database Audit Log Filter Settings

☑ Enable Audit Log Debug Audit Level: Schema Only

Output Settings

☑ Enable Audit Log Rotation

Maximum No. of Files*: 40

No. of Files Deleted on Log Rotation*: 20

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Physical Security

Cisco Physical Security solutions provide broad capabilities in video surveillance, IP cameras, electronic access control, and groundbreaking technology that converges voice, data, and physical security in one modular platform. Cisco Physical Security solutions enable customers to use the IP network as an open platform to build more collaborative and integrated physical security systems while preserving their existing investments in analog-based technology. As customers converge physical security infrastructures and operations and begin using the IP network as the platform, they can gain significant value through rapid access to relevant information and interoperability between systems. This creates a higher level of situational awareness and allows intelligent decisions to be made more quickly.

Cisco Video Surveillance

Video surveillance technology provides security monitoring capabilities within a store environment. Video surveillance for loss prevention can now be extended into the area of protecting the cardholder data environment.

As the core component of Cisco's video surveillance software portfolio, the Cisco Video Surveillance Media Server offers the power and flexibility to meet a diverse range of video surveillance requirements. The media server:

- Uses IP technology to provide outstanding scalability in terms of sites, cameras, viewers, and storage
- Delivers low-latency, high-quality, event-tagged video
- Supports a broad range of cameras, codecs (such as JPEG, and MPEG-4, and H.264), viewing platforms, and network topologies
- Archives at various frame rates, durations, and locations

Quickly and effectively configure and manage video throughout your enterprise with the Cisco Video Surveillance Operations Manager (VSOM). Working in conjunction with the Cisco Video Surveillance Media Server and Cisco Video Surveillance Virtual Matrix, the Operations Manager meets the diverse needs of administrators, systems integrators, and operators by providing:

- A web-based toolkit for configuration, management, display, and control of video from a wide variety of both Cisco and third-party surveillance endpoints
- Management of a large number of Cisco Video Surveillance Media Servers, Virtual Matrixes, cameras, and users
- Flexible video recording options including motion-based, scheduled, and event-based
- Comprehensive control of users and user roles including scheduling of operator shifts, event filters, and user-specific video views
- Detailed activity reports and system audit

Table 5-6 PCI Assessment Summary—Cisco Video Surveillance

Models Assessed	
Cisco Video Surveillance Manager version 6.3.1	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 9	9.1, 9.1.1
PCI 10	10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 104.3, 10.5, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary function of video surveillance is to monitor physical access to sensitive areas within the cardholder data environment (9.1.1).

Table 5-6 lists the component assessment details for the Cisco Video Surveillance solution.

Table 5-7 Component Capability Assessment—Cisco Video Surveillance

Cisco Video Surveillance	
PRIMARY FUNCTION	**Requirement 9 (9.1.1)**
Monitor physical access to sensitive areas within the cardholder environment.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- Ensure that cameras are positioned to monitor servers or systems within the cardholder data environment.
- Cameras should be appropriately positioned to identify personnel accessing these systems.
- Ensure adequate storage of video for three months.

For more information, see the Cisco IP Video Surveillance Guide at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/IPVS/IPVS_DG/IPVSchap4.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2—***Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The Cisco Video Surveillance Manager includes only the required services, ports, applications, and access required for standard operation of the system. Use the Cisco Video Surveillance Operations Manager Secure Login feature, found within the Administrative Settings, to enable and force secure HTTPS application login.

- **PCI 2.2.4—***Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco Video Surveillance Manager and Multiservices Platform contain only the required components needed to run the applications. If additional network, software, or platform security customization is required, consult *Securing Video Surveillance Manager: Best Practices and Recommendations* at the following URL: http://www.cisco.com/en/US/docs/security/physical_security/video_surveillance/network/design/bestprac_4_1_6_1.pdf

- **PCI 2.3—***Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The Cisco Video Surveillance Manager uses SSL for web-based administration and operator access, and uses SSH for remote terminal access. Use the Cisco Video Surveillance Operations Manager Secure Login feature, found within the Administrative Settings, to enable and force secure HTTPS application login. SSH access should be used to securely login to the VSM host.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Video Surveillance Operations Manager. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of requirement 7 were met using VSOM's Role-based Access Control (RBAC) system to logically group each user within a role based on their need to know. This restricts unauthorized access and usage of system components. The VSOM RBAC allows granular access control for each system component, including devices such as servers, cameras, and encoders, along with application-level functionality of accessing these resources.

This configuration was used to address the following individual requirements.

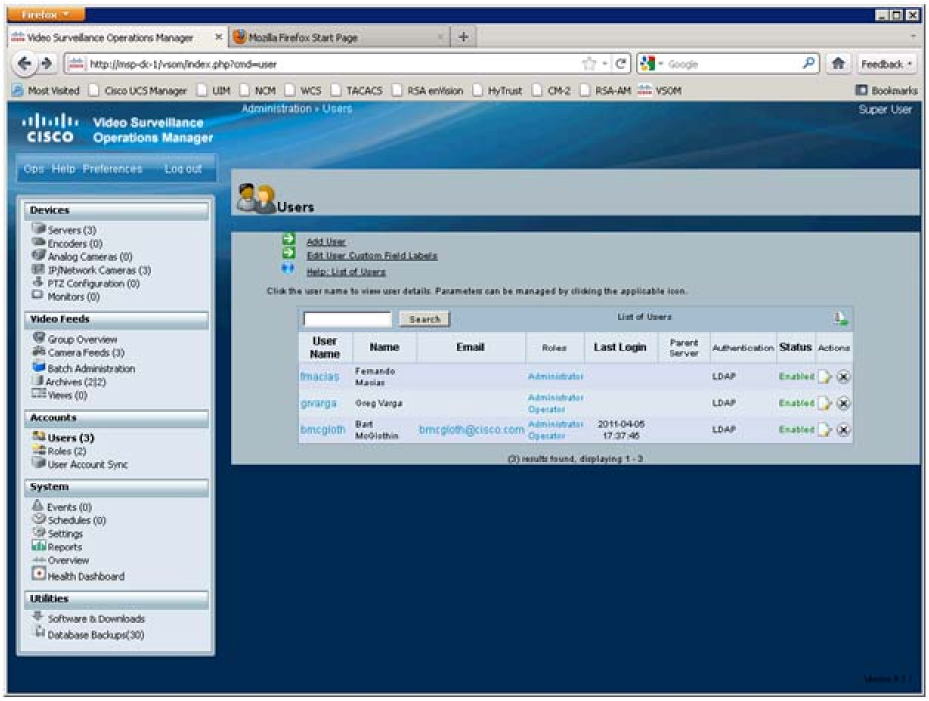
- **PCI 7.1—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:*
  - **PCI 7.1.1—***Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
  - **PCI 7.1.2—***Assignment of privileges is based on individual personnel's job classification and function*
  - **PCI 7.1.3—***Requirement for a documented approval by authorized parties specifying required privileges.*
  - **PCI 7.1.4—***Implementation of an automated access control system*

- **PCI 7.2—***Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:*
  - **PCI 7.2.1—***Coverage of all system components*
  - **PCI 7.2.2—***Assignment of privileges to individuals based on job classification and function*
  - **PCI 7.2.3—***Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  The role configuration menu in Video Surveillance Operations Manager server allows specifying the assignment of privileges based on the role description. No systems access is permitted without an account.

  Individual users and roles are created locally and authentication directed to LDAP, as shown in Figure 5-10.

Figure 5-10 VSOM Users Authenticate to LDAP Service



Users

Click the user name to view user details. Parameters can be managed by clicking the applicable icon.

List of Users

User Name	Name	Email	Roles	Last Login	Parent Server	Authentication	Status	Actions
fmacias	Fernando Macias		Administrator			LDAP	Enabled	
gvarga	Greg Varga		Administrator Operator			LDAP	Enabled	
bmcgloth	Bart McGlothin	bmcgloth@cisco.com	Administrator Operator	2011-04-05 17:37:46		LDAP	Enabled	

(3) results found, displaying 1 - 3

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing LDAP connectivity for AAA services and Microsoft Active Directory for user account services. Configure AAA services via LDAP, as shown below.

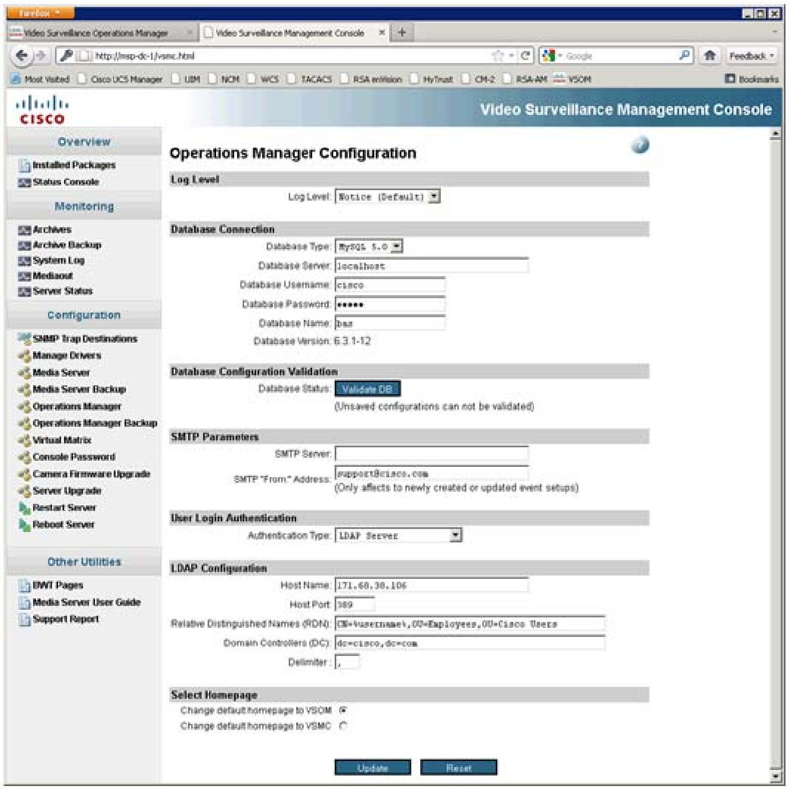
- **PCI 8.1—***Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2—***In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*

   - *Something you are, such as a biometric*

- **PCI 8.4—***Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5—***Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9—***Change user passwords at least every 90 days.*
- **PCI 8.5.10—***Require a minimum password length of at least seven characters.*
- **PCI 8.5.11—***Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12—***Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13—***Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14—***Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Using the Video Surveillance Management Console, configure LDAP as specified in the installation guide. Figure 5-11 shows the LDAP configuration implemented for validation.

Figure 5-11 VSOM LDAP Configuration



Operations Manager Configuration

Log Level

Log Level: Notice (Default)

Database Connection

Database Type: MySQL 5.0
Database Server: localhost
Database Username: cisco
Database Password: •••••
Database Name: bas
Database Version: 6.3.1-12

Database Configuration Validation

Database Status: Validate DB
(Unsaved configurations can not be validated)

SMTP Parameters

SMTP Server:
SMTP "From:" Address: support@cisco.com
(Only affects to newly created or updated event setups)

User Login Authentication

Authentication Type: LDAP Server

LDAP Configuration

Host Name: 171.68.38.106
Host Port: 389
Relative Distinguished Names (RDN): CN=%username%,OU=Employees,OU=Cisco Users
Domain Controllers (DC): dc=cisco,dc=com
Delimiter: ,

Select Homepage

Change default homepage to VSOM ●
Change default homepage to VSMC ○

- **PCI 8.5.15—***If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

Cisco VSOM has a minimum session timeout of 30 minutes in the configuration for the version validated. Administration time limits would need to be enabled systemically through an active directory policy to the admin workstation desktops, locking them when there is no activity after 15 minutes.

Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1—***Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.*
- **PCI 9.1.1—***Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*

  Physical access to sensitive areas and cardholder data is restricted by solutions in video surveillance management and IP cameras by securing data center facilities and cashier areas within retail stores. This includes video recording options for flexible configuration of video recording archives and low-latency, high-quality, event-tagged video. Also available is the following:

  - A web-based interface for configuration, management, display, and control of video from a wide variety of surveillance and monitoring endpoints
  - Management of a large number of video surveillance media servers, video walls, cameras, and users
  - Comprehensive control of users and user roles including scheduling of operator shifts, event filters, and user-specific video views
  - Detailed activity reports and system audit

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco VSOM is able to track and monitor all administrative user access and events.

Cisco VSOM uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*

  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*
- **PCI 10.4—***Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).*
  - **PCI 10.4.2—***Time data is protected.*
  - **PCI 10.4.3—***Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Network Time Protocol (NTP) is supported and must be enabled within both the IP cameras and Video Surveillance Manager.

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects information from all devices to ensure the integrity and correlation of events.

Requirement 10.5 was met using the integrated Log Backup functionality to send the logging data to the RSA enVision server.

- **PCI 10.5—***Secure audit trails so they cannot be altered.*
  - **PCI 10.5.1—***Limit viewing of audit trails to those with a job-related need.*
  - **PCI 10.5.2—***Protect audit trail files from unauthorized modifications.*
  - **PCI 10.5.3—***Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
  - **PCI 10.5.5—***Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  The following configuration script was implemented to send the local log files to the RSA enVision server to be secured and the integrity established:

```
Directory:  /etc/cron.daily
Filename:  ftp-backup-files.cron

#!/bin/sh
FTP_USER=anonymous
FTP_PASS='vsom@cisco.com'
localDIR="/usr/BWhttpd/bas/db/backups"
serverDIR="/vsom_backup/"

cd $localDIR
ftp -n -i 192.168.42.124   <<EOF
user $FTP_USER $FTP_PASS
binary
cd $serverDIR
mput VSOM_MSP-DC-1_backup_20$(date +%y%m%d)*.tar.gz
quit
EOF
exit 0
```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

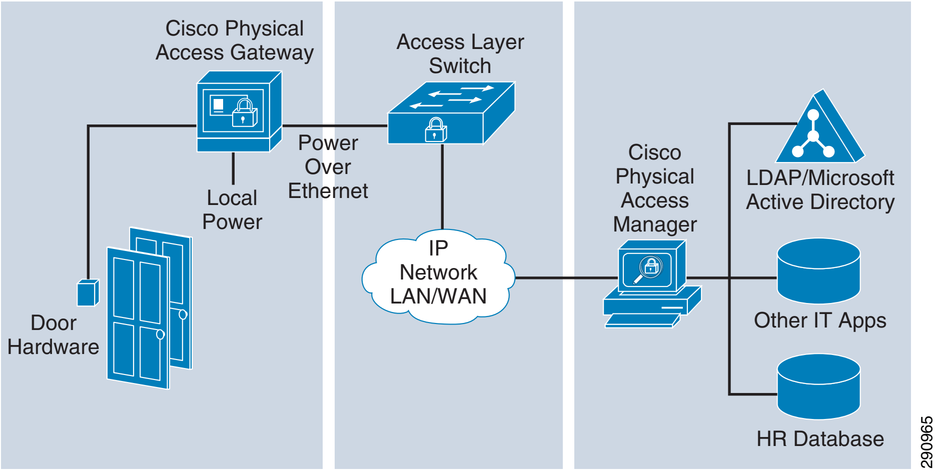
Cisco Physical Access Control

Cisco Physical Access Control allows retailers to secure their physical doors and locations. Cisco Physical Access Control addresses specific PCI requirements by providing:

- Secure access to the server by supporting secure protocols such as HTTPS and also securing the accounts using strong passwords
- Role-based access to the system by making use of profiles that can restrict access to the modules, depending on the roles
- Automated backup of events to a centralized server
- Ability to archive audit reports on a centralized server

Cisco Physical Access Control is a comprehensive IP-based solution that uses the IP network as a platform for integrated security operations (see Figure 5-12). It works with existing card readers, locks, and biometric devices and is integrated with Cisco Video Surveillance Manager (VSM) and with Cisco IP Interoperability and Collaboration System (IPICS).

Figure 5-12 Scalable, Modular Architecture



Cisco Physical Access Control has two components:

- The hardware component, Cisco Physical Access Gateway, provides a modular and scalable platform to connect readers, inputs, and outputs to the system. The gateway scales from a single door to thousands of doors at a fixed cost per door.
- The software component, Cisco Physical Access Manager, manages the hardware, monitors activity, enrolls users, and integrates with IT applications and data stores.

Table 5-8 PCI Assessment Summary—Cisco Physical Access Manager

Models Assessed	
Cisco Physical Access Manager version 1.2.0	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary function of the CPAM appliance is to configure, manage, monitor, and report on the physical doors and door hardware, protecting sensitive areas within the cardholder data environment (9.1).

Table 5-8 lists the component assessment details for Cisco Physical Access Control.

Table 5-9 Component Capability Assessment—Cisco Physical Access Control

Cisco Physical Access Control	
PRIMARY FUNCTION	**Requirement 9 (9.1)**
Limit and monitor physical access to sensitive areas within the cardholder data environment.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

Best practices are as follows:

- Use high availability for Cisco Physical Access Manager (PAM) servers.
- Map each store location and identify the following:
  - Actual doors and modules
  - Door devices and module ports
- Use backup power supply for servers, modules, and devices.
- Cisco PAM was implemented following the Cisco Physical Access Manager Appliance User Guide, Release 1.2.0: http://www.cisco.com/en/US/docs/security/physical_security/access_control/cpam/1_2_0/english/user_guide/cpam_1_2_0.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2—***Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

The Cisco PAM appliance can be configured to disable unsecure protocols. To disable unsecure protocols, you must edit one of the configuration files on the Cisco PAM appliance. The step-by-step instructions are as follows:

- SSH into the Cisco PAM server
- sudo su
- Enter the *cpamadmin* password
- /etc/init.d/cpamadmin stop
- Comment out a configuration from the file /opt/cisco/cpam/apache-tomcat/conf/server.xml.

Remove or comment the snippet below.

```
<Connector executor="tomcatThreadPool"
           port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

```
/etc/init.d/cpamadmin start
```

When you try to launch the web UI using HTTP, you see “Page cannot be displayed”.

- **PCI 2.2.4—***Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco PAM appliance operating system includes only the components needed to run the application.

- **PCI 2.3—***Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  On the Cisco PAM appliance, SSL is enabled by default. All the communication between the Cisco PAM client and the gateway is encrypted using the 128-bit AES encryption. Console access to Cisco PAM is through SSH.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco PAM. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

To meet all of the requirements listed below, the PCI solution for retail uses a centralized user database in the Active Directory, which is linked via LDAP, RADIUS, and TACACS+ services. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. Cisco Physical Access Manager connects to this resource via LDAP to address the following individual requirements:

- **PCI 7.1**—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:*
  - **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
  - **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
  - **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
  - **PCI 7.1.4**—*Implementation of an automated access control system*

  Role-based access can be configured on Cisco PAM by making use of profiles. Profiles are pre-defined sets of access privileges that define the Cisco PAM modules and commands available to a user. For example, users that should have all privileges can be assigned to the Administrators profile.

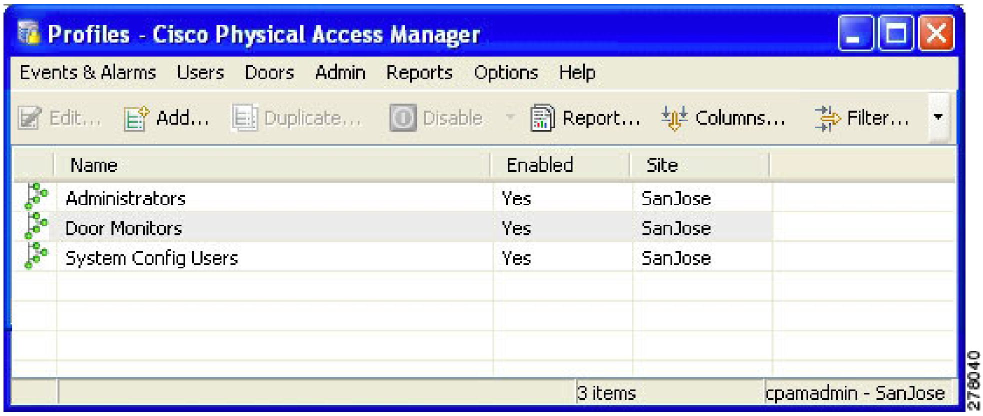
Note The Administrator profile is read-only and cannot be changed.

To create profiles, do the following:

Step 1 Select **Profiles** from the Users menu.

Step 2 To add a profile, choose **Add**. (See Figure 5-13.)

Figure 5-13 Profiles Module Main Window



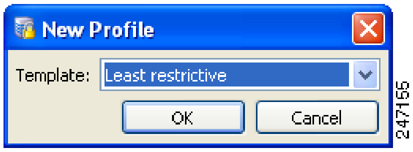
Name	Enabled	Site
Administrators	Yes	SanJose
Door Monitors	Yes	SanJose
System Config Users	Yes	SanJose

Note To modify an existing profile, select the entry and choose **Edit**. To remove a profile, select the entry and choose **Delete**. The Administrator profile is read-only and cannot be changed.

Step 3 Select a Profile template that most closely matches the desired level of user access, as shown in Figure 5-14:

- Default—A basic set of privileges is set.
- Most Restrictive—No privileges are set.
- Least Restrictive—All privileges are set.

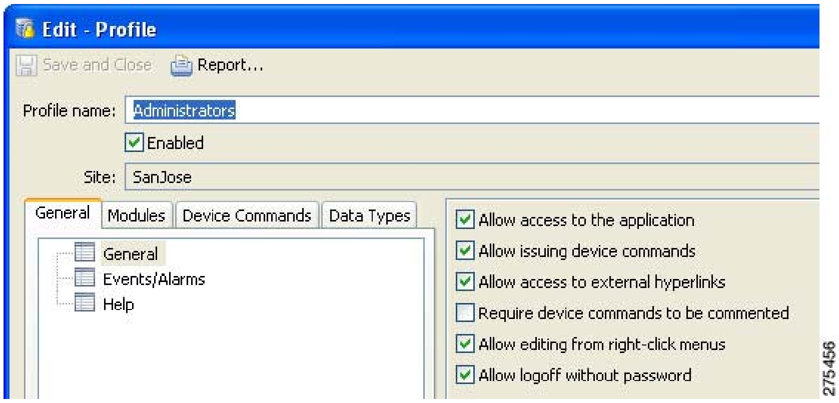
Figure 5-14 Profile Templates


New Profile

Template: Least restrictive

Step 4 Enter the basic profile settings, as shown in Figure 5-15.

Figure 5-15 Profile—General Tab


Edit - Profile

Profile name: Administrators

☑ Enabled

Site: SanJose

☑ Allow access to the application
☑ Allow issuing device commands
☑ Allow access to external hyperlinks
□ Require device commands to be commented
☑ Allow editing from right-click menus
☑ Allow logoff without password

- Profile name—Enter a descriptive name for the profile.
- Enabled—Select the check box to enable the profile, or deselect the box to disable the profile.
- Partition—Select the partition from the drop-down menu.

Step 5 Click the **General** tab to define the basic profile properties. Click the checkbox next to each field to enable or disable the privilege, as described in Table 5-10.

Table 5-10 General Settings—Profile Module

Field	Description
General	
Allow access to the application	Allows access to the application.
Allow issuing device commands	Allows user to issue device commands directly to hardware.
Allow access to external hyperlinks	Allows access to external hyperlinks.
Require device commands to be commented	Requires the user to enter a comment with each device command issued in the system.
Allow editing from right-click menus	Allows access to the right-click the Edit menu.

Table 5-10 General Settings—Profile Module (continued)

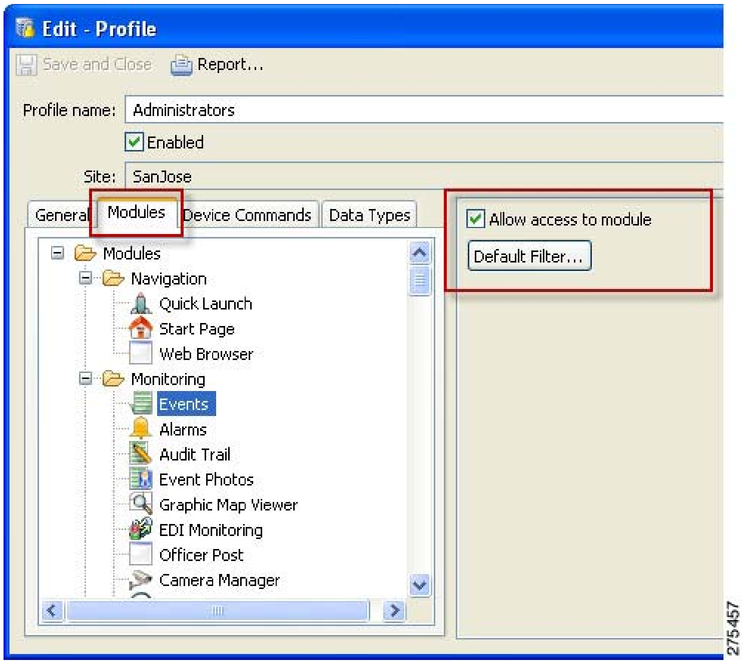
Allow logoff without password	Allows user to logoff without a password.
Events/Alarms: Alarm Annotations (Ack., Clear, Comment)	
Allow annotations	Allows user to acknowledge, clear, and comment alarms. Click the **Filter** button to define the events that trigger the action.
Allow multiple annotations	Allows the user to acknowledge, clear, and comment multiple alarms at one time.
Allow clearing of unacknowledged alarms	Allows the user to clear unacknowledged alarms from active devices.
Allow clearing of active device alarms	Allows the user to clear alarms from active devices.
Events/Alarms—On new alarms	
Open Alarms Module	The **Alarms** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Open Manage Alarm window	The **Alarms** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Open graphic map	The **Graphic Map** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show recorded video	Displays recorded video with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show live video	Displays live video with new system alarms. Click the **Filter** button to define the events that trigger the action.
Help—Defines access to the various help systems	
Allow access to help documentation	Allows access to help documentation.
Enable context menu in help browser	Allows the user to view the help context menu.
Allow access to help PDF	Allows the user to access the help PDF. Adobe PDF viewer is required.

Step 6 Click the **Modules** tab to define the modules accessible to the profile, as shown in Figure 5-16.

a. Select a Cisco PAM module.

b. Select **Allow access to module** to enable access to the module.

Figure 5-16 Profile—Modules Tab



Profile name: Administrators

☑ Enabled

Site: SanJose

☑ Allow access to module

c. (Optional) Use the **Default Filter** with modules such as Event, Badge, and Personnel to define the filter applied when a user opens the module.

For example, to create a profile with access to the Events module that displays events for a specific door by default, complete the following sample steps:

1. Create a profile with access to the Events module, as described in the previous steps.

2. Click **Default Filter**, as shown in Figure 5-16.

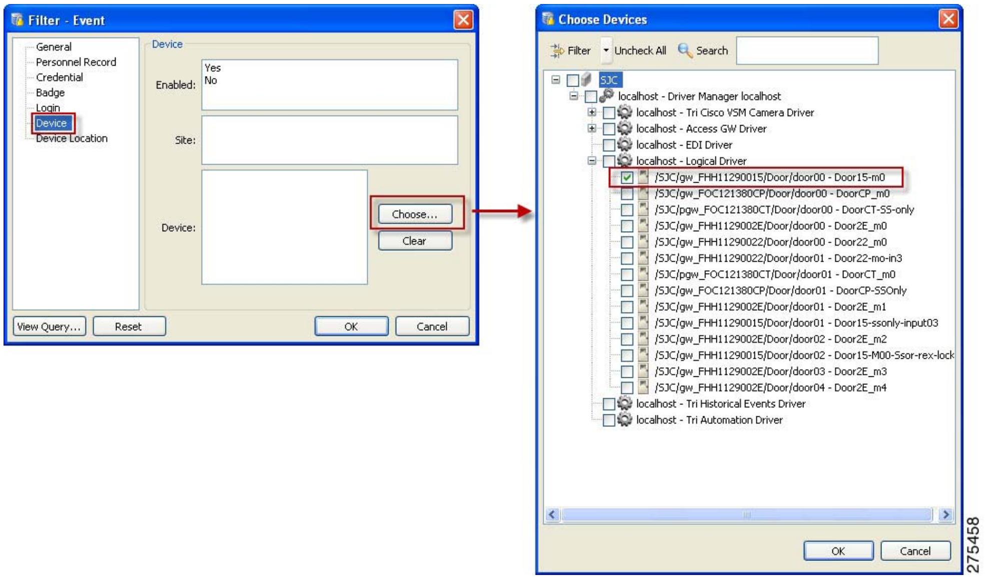
3. Select the **Device** tab, as shown in Figure 5-17.

4. Click **Choose**.

In the Choose Devices window, expand the Logical Driver device tree and select a door (Figure 5-17).

5. Click **OK** to save the changes and close the windows.

Figure 5-17 Default Filter: Device Settings



Filter - Event

General
Personnel Record
Credential
Badge
Login
Device
Device Location

Device

Enabled: Yes
No

Site:

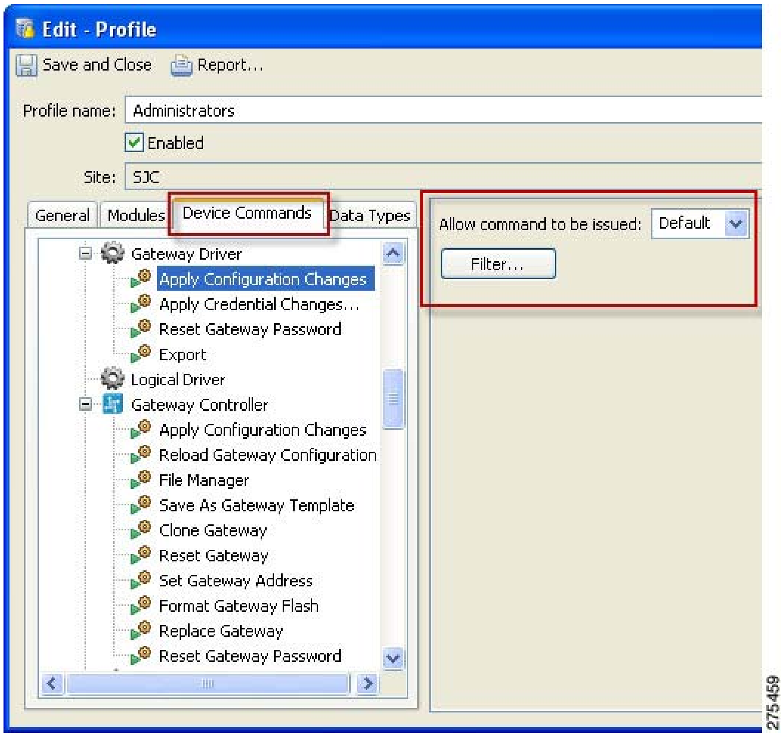
Device:

Choose Devices

□ SJC
□ localhost - Driver Manager localhost
□ localhost - Tri Cisco VSM Camera Driver
□ localhost - Access GW Driver
□ localhost - EDI Driver
□ localhost - Logical Driver
☑ /SJC/gw_FHH11290015/Door/door00 - Door15-m0
□ /SJC/gw_FOC121380CP/Door/door00 - DoorCP_m0
□ /SJC/pgw_FOC121380CT/Door/door00 - DoorCT-SS-only
□ /SJC/gw_FHH1129002E/Door/door00 - Door2E_m0
□ /SJC/gw_FHH11290022/Door/door00 - Door22_m0
□ /SJC/gw_FHH11290022/Door/door01 - Door22-mo-in3
□ /SJC/pgw_FOC121380CT/Door/door01 - DoorCT_m0
□ /SJC/gw_FOC121380CP/Door/door01 - DoorCP-SSOnly
□ /SJC/gw_FHH1129002E/Door/door01 - Door2E_m1
□ /SJC/gw_FHH11290015/Door/door01 - Door15-ssonly-input03
□ /SJC/gw_FHH1129002E/Door/door02 - Door2E_m2
□ /SJC/gw_FHH11290015/Door/door02 - Door15-M00-Ssor-rex-lock
□ /SJC/gw_FHH1129002E/Door/door03 - Door2E_m3
□ /SJC/gw_FHH1129002E/Door/door04 - Door2E_m4
□ localhost - Tri Historical Events Driver
□ localhost - Tri Automation Driver

Step 7 Click the **Device Commands** tab to define the hardware configuration commands available to the user (see Figure 5-18).

Figure 5-18 Profile—Device Commands Tab



Edit - Profile

Profile name: Administrators

☑ Enabled

Site: SJC

Gateway Driver
Apply Configuration Changes
Apply Credential Changes...
Reset Gateway Password
Export
Logical Driver
Gateway Controller
Apply Configuration Changes
Reload Gateway Configuration
File Manager
Save As Gateway Template
Clone Gateway
Reset Gateway
Set Gateway Address
Format Gateway Flash
Replace Gateway
Reset Gateway Password

Allow command to be issued: Default

a. Expand or collapse the list of commands for a device.

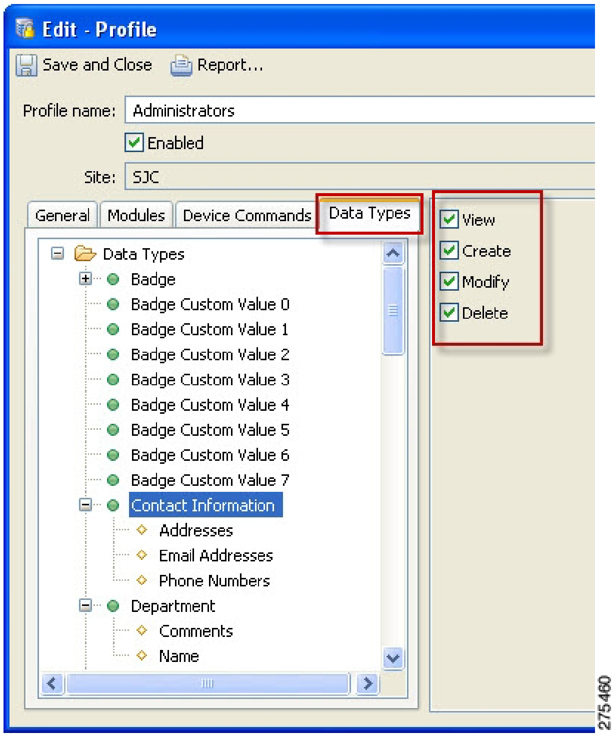
b. Highlight a command.

c. Select the following options:

- Allow command to be issued:
  - Default—If user has access to issue device commands, the command access is enabled by default.
  - No—Denies access to the command.
  - Yes—Allows access to the command.
- Filter—Apply a filter to limit the devices for the command.

Step 8 Click the **Data Types** tab to define the data available to the profile, as shown in Figure 5-19.

Figure 5-19 Profile—Data Types Tab



Profile name: Administrators

☑ Enabled

Site: SJC

☑ View
☑ Create
☑ Modify
☑ Delete

a. Select a module and the type of data in the list.

b. To restrict the data, click the check boxes for the properties listed in Table 5-11.

Table 5-11 Profile—Data Types

Field	Description
View	Allows the user to view the selected data type.
Create	Allows the user to add and create the selected data types.
Modify	Allows the user to modify existing data.
Delete	Allows the user to delete data.
Default Filter...	Allows the user to apply a default filter to limit objects from view.

Step 9 Click **Save and Close** to save the profile settings.

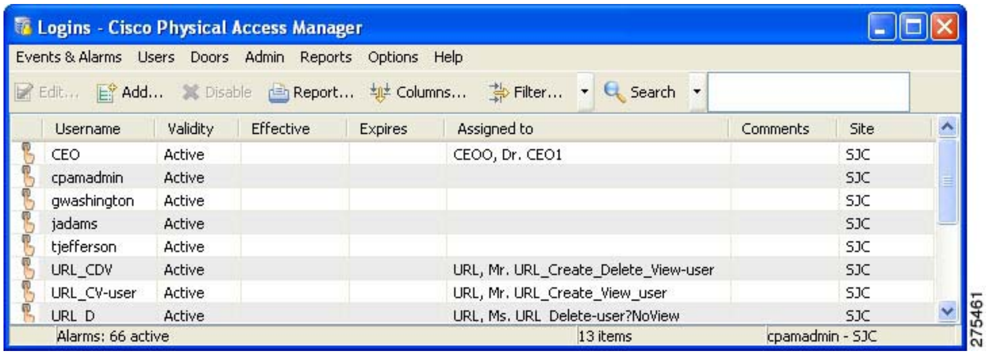
Step 10 Assign the profile to one or more Cisco PAM operators using the Logins module. (See the following section).

Creating User Login Accounts and Assigning Profiles

To give users access to Cisco PAM functionality, create a login account and assign one or more access profiles to the username.

Step 1 Select **Logins** from the Users menu. The main window (Figure 5-20) lists all the usernames in the system.

Figure 5-20 Logins Module Main Window



Username	Validity	Effective	Expires	Assigned to	Comments	Site
CEO	Active			CEOO, Dr. CEO1		SJC
cpamadmin	Active					SJC
gwashington	Active					SJC
jadams	Active					SJC
tjefferson	Active					SJC
URL_CDV	Active			URL, Mr. URL_Create_Delete_View-user		SJC
URL_CV-user	Active			URL, Mr. URL_Create_View_user		SJC
URL_D	Active			URL, Ms. URL_Delete-user?NoView		SJC

Alarms: 66 active 13 items cpamadmin - SJC

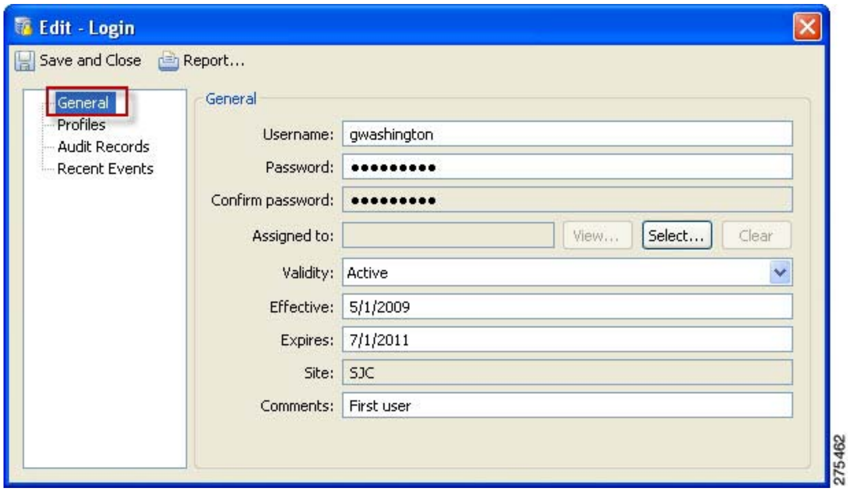
Step 2 To add a login, choose **Add**.

- To modify an existing login, select the entry and choose **Edit**.
- To remove a login, select the entry and choose **Delete**.

Note Most properties of the *cpamadmin* login are read-only.

Step 3 Complete fields in the General tab, as shown in Figure 5-21. Table 5-12 describes the field properties.

Figure 5-21 Logins Module—General Tab



Username: gwashington
Password: ●●●●●●●●●
Confirm password: ●●●●●●●●●
Assigned to:
Validity: Active
Effective: 5/1/2009
Expires: 7/1/2011
Site: SJC
Comments: First user

Note The Username, Password, and Confirm password fields are required.

Table 5-12 General Tab Fields

Field	Description
Username	Required—The username of the login.
Password	Required—Password to access the system.
Confirm password	Required—The value must be entered exactly as it was in the Password field.
Assigned to	The personnel record the login is assigned to. If the login is for an operator already entered in the Personnel module, click the **Select...** button. For more information on adding personnel to the system, see Chapter 8, “Configuring Personnel and Badges” of the CPAM User guide.
Validity	Active or Inactive—Only active accounts can access the system.
Effective	The beginning date the user can log in—If left blank, the user can log in immediately.
Expires	The day the login expires and access is denied—If left blank, access is allowed indefinitely.
Site	Read-only—A site is a single instance of a Cisco PAM database.
Comments	Comments or notes about the login.

Step 4 Assign access privileges for the login:

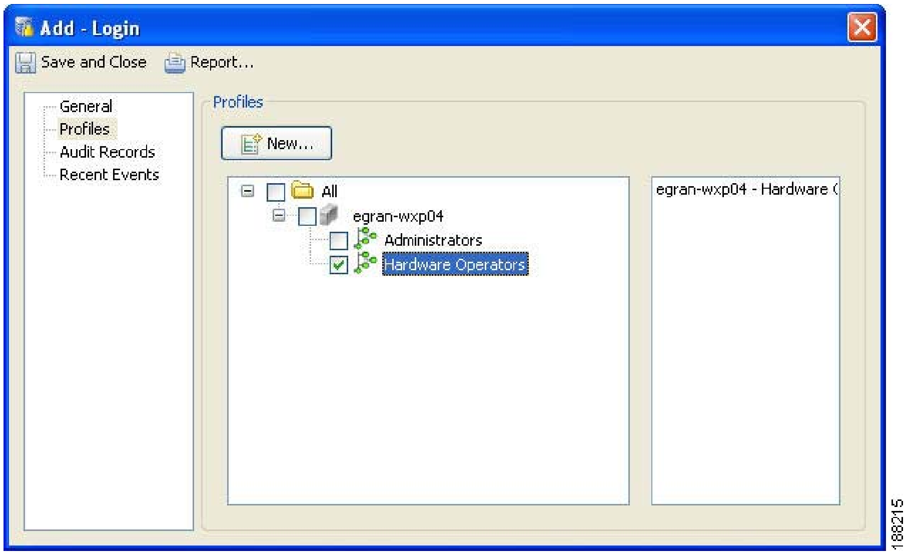
a. Select the **Profiles** tab, as shown in Figure 5-22.

b. Select the checkbox next to each profile to enable or disable access rights as defined by the access profile. For more information, see Defining User Profiles for Desktop Application Access.

c. Click **Save and Close** to save the changes and close the window.

Tip To create a new access profile, click the New button to open the Profiles module and refer to Defining User Profiles for Desktop Application Access.

Figure 5-22 Assigning One or More Profiles



□ All
□ egran-wxp04
□ Administrators
☑ Hardware Operators

egran-wxp04 - Hardware (

Step 5 To verify the changes, log off and then log in with the new username and password. Verify that you can access the modules and functions specified by the assigned profiles.

- **PCI 7.2—***Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:*
  - **PCI 7.2.1—***Coverage of all system components*
  - **PCI 7.2.2—***Assignment of privileges to individuals based on job classification and function*
  - **PCI 7.2.3—***Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco PAM has a default policy of "Deny-all". If a specific badge has to get access to certain set of doors, an access policy must be created.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance with the sub-requirements in this section was achieved within the solution by implementing LDAP connectivity for AAA services and Microsoft Active Directory for user account services. Configure AAA services via LDAP, as shown in Requirement 8.2.

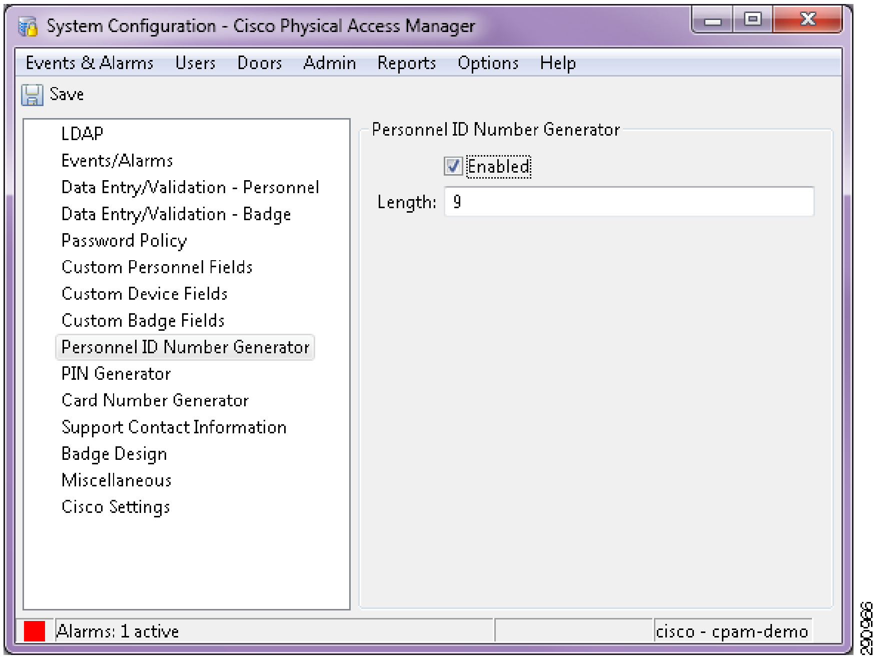
- **PCI 8.1—***Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco PAM integrates with Microsoft Active Directory (MS AD) to pull user information into CPAM. MS AD supports creation of unique ID for users. Cisco PAM has an option to generate a unique number for users using the Personnel ID Number Generator. It is disabled by default. Following are the instructions to enable and use this feature.

Step 1 On the Cisco PAM client application, open the System Configuration module by clicking **Admin -> System Configuration**.

Step 2 Click **Personnel ID Number Generator** on the left (see Figure 5-23) and check **Enabled**. Click **Save**.

Figure 5-23 Using the Personnel ID Number Generator



Personnel ID Number Generator

☑ Enabled

Length: 9

Alarms: 1 active

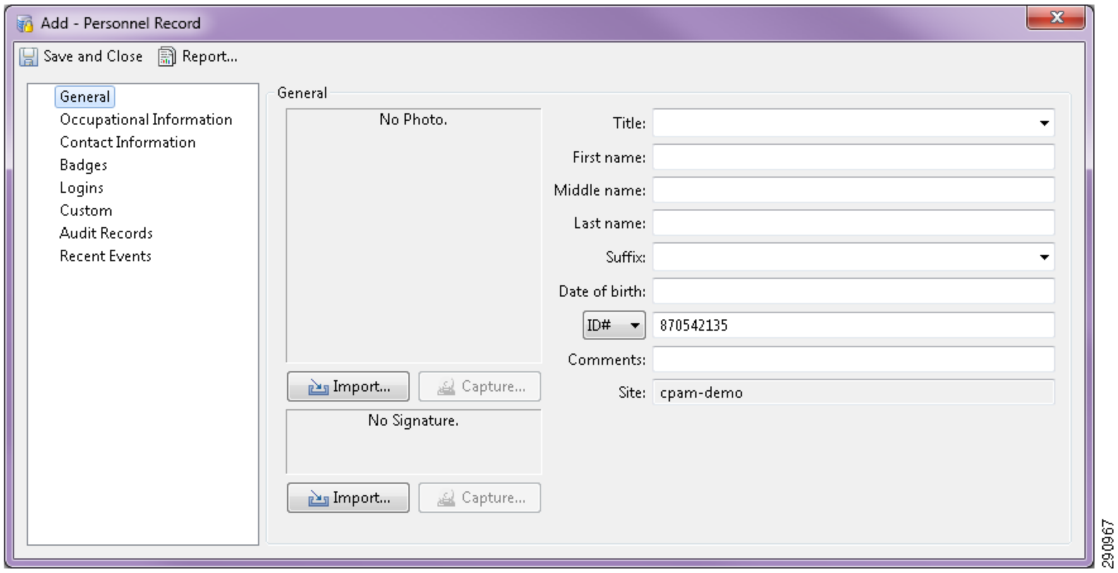
cisco - cpam-demo

Step 3 Log out and log back into the Cisco PAM client to get the Personnel ID Number Generator featured working.

Step 4 Click on **Users -> Personnel**.

Step 5 Click **Add**. You should see a unique number generated automatically in the ID# field, as shown in Figure 5-24.

Figure 5-24 Unique ID Number



No Photo.

No Signature.

Title:

First name:

Middle name:

Last name:

Suffix:

Date of birth:

ID# 870542135

Comments:

Site: cpam-demo

- **PCI 8.2—***In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Cisco PAM supports authentication through LDAP. Because LDAP supports this feature, Cisco supports the methods listed above.

Configuring LDAP User Authentication on Cisco PAM

To authenticate users using a Lightweight Directory Access Protocol (LDAP) server, do the following:

1. Configure the LDAP Server
2. Create the LDAP User Account in Cisco PAM

Configure the LDAP Server

Enter the LDAP server settings to configure the LDAP server connection and user authentication, as described in the following steps.

Step 1 Select **System Configuration** from the Admin menu, and then select the **LDAP** tab.

Step 2 Enter the LDAP user authentication settings. The LDAP configuration depends on the authentication mode:

- User principal name (recommended method)—The user principal name is unique in the organization.
- sAMAccountName—The sAMAccount username is unique only in the search domain.

LDAP uses a principle to authenticate. The principle is formed from the username: prefix + username + suffix. The exact format of the principle varies based on the type of LDAP server, and the domain.

For OpenLDAP, the prefix should be: uid=
The suffix should be changed to reflect the actual domain.
So for my-domain.com, this would be:
,dc=my-domain, dc=com

For more information, see the following:

- LDAP Example: User Principal Name
- LDAP Example: sAMAccountName

Step 3 Enter the other LDAP server settings, as listed in Table 5-13.

Table 5-13 LDAP System Configuration Settings

Field	Description
Enable LDAP	Click the checkbox to enable or disable LDAP support.
LDAP server URL	URL of LDAP server, must begin with ldap:// Example: ldap://192.168.1.1:389 **Note** 389 is the port number.
Principle suffix	Appended to the username for authentication. See above.

Table 5-13 LDAP System Configuration Settings (continued)

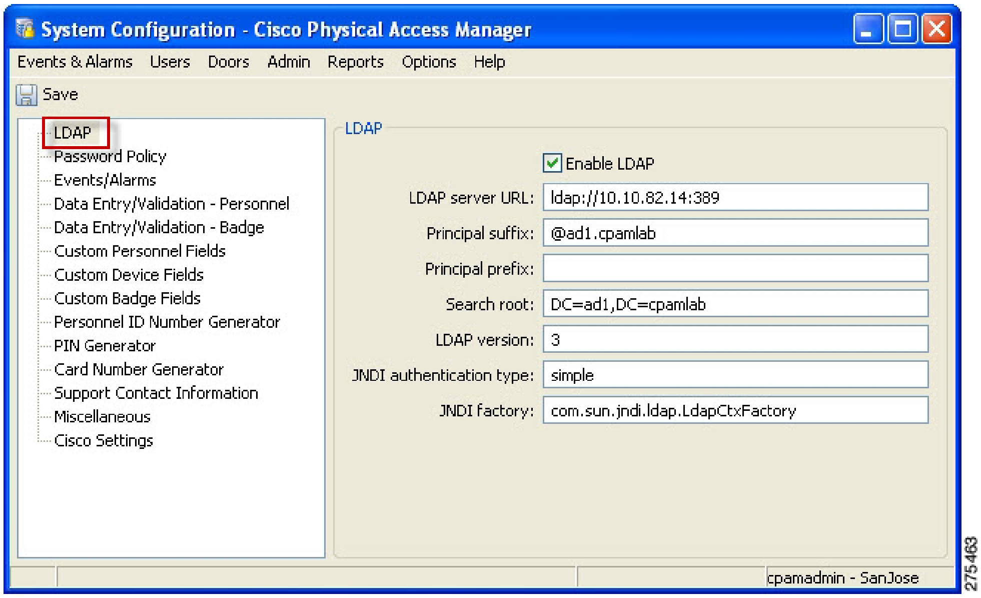
Principle prefix	Prepended to the username for authentication. See above.
Search root	LDAP search root. The search root is the node in the LDAP tree, the subtree under which the user account should be found. • For Active Directory, the dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com: cn=Users, dc=my-domain, dc=com. • For OpenLDAP, the 2 dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com:dc=my-domain,dc=com.
LDAP version	An advanced setting that generally should be left unchanged.
JNDI authentication type	An advanced setting that generally should be left unchanged as simple.
JNDI factory	An advanced setting that generally should be left unchanged as com.sun.jndi.ldap.LdapCtxFactory

Step 4 Log out and log back in to the Cisco PAM application to enable the changes (select **Logout** from the Options menu).

LDAP Example—User Principal Name

In the example shown in Figure 5-25, the user principal name is *cpsm.user@ad1.cpamlab*. The Cisco PAM user login must be the same (*cpsm.user*).

Figure 5-25 User Principal LDAP Configuration Example



LDAP

☑ Enable LDAP

LDAP server URL: ldap://10.10.82.14:389

Principal suffix: @ad1.cpamlab

Principal prefix:

Search root: DC=ad1,DC=cpamlab

LDAP version: 3

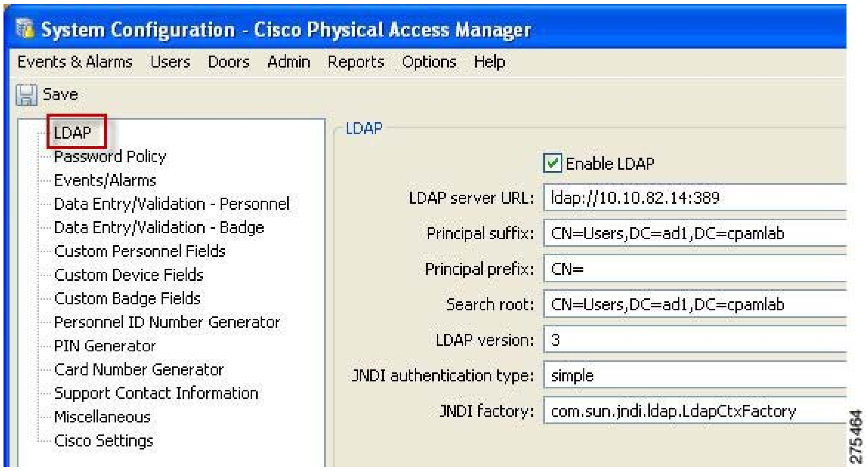
JNDI authentication type: simple

JNDI factory: com.sun.jndi.ldap.LdapCtxFactory

LDAP Example—sAMAccountName

In the example shown in Figure 5-26, the user login is the same as the samaccount name (*cpsmuser*).

Figure 5-26 sAMAccountName—LDAP Configuration Example



☑ Enable LDAP

LDAP server URL: ldap://10.10.82.14:389

Principal suffix: CN=Users,DC=ad1,DC=cpamlab

Principal prefix: CN=

Search root: CN=Users,DC=ad1,DC=cpamlab

LDAP version: 3

JNDI authentication type: simple

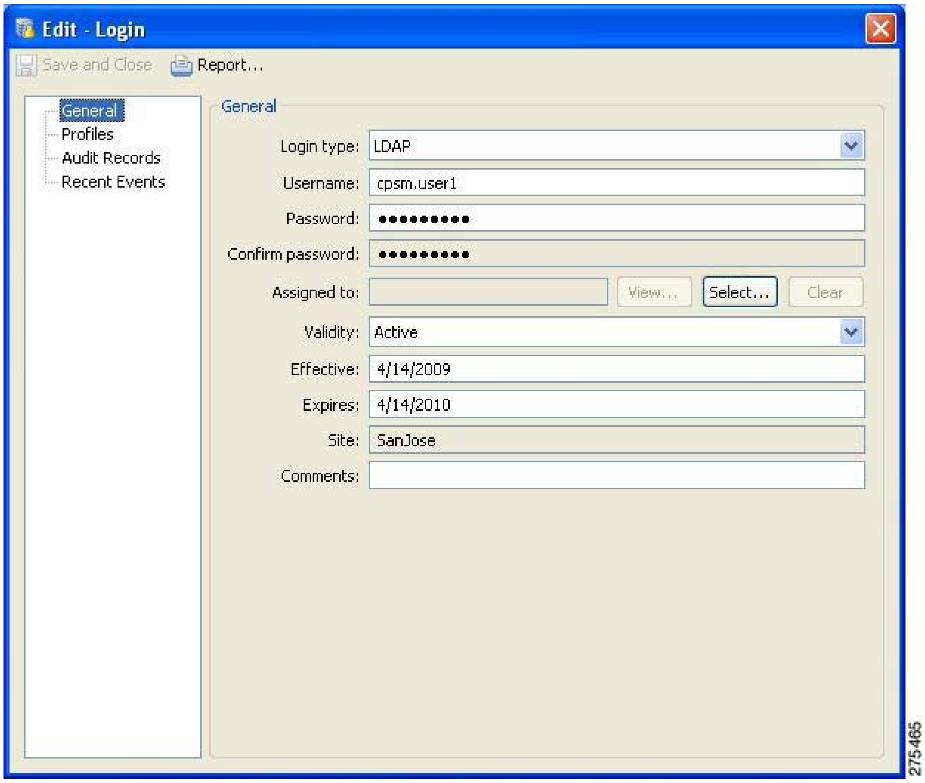
JNDI factory: com.sun.jndi.ldap.LdapCtxFactory

Creating the LDAP User Account in Cisco PAM

Create the user account to be authenticated using an LDAP server with the following steps.

Step 1 Select **Logins** from the Users menu. (See Figure 5-27.)

Figure 5-27 Login Window: LDAP Login Type



Login type: LDAP

Username: cpsm.user1

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

Assigned to:

Validity: Active

Effective: 4/14/2009

Expires: 4/14/2010

Site: SanJose

Comments:

Step 2 Click **Add**, or select an existing login and click **Edit**.

Step 3 Select the Login type **LDAP**. The Login type field appears only if LDAP was enabled and the Cisco PAM application was restarted (see Configure the LDAP Server).

Step 4 Enter the username, password, and other settings for the LDAP login. See Creating User Login Accounts and Assigning Profiles.

Note Although a password must be entered for all user Login records, it is not used for LDAP authentication. LDAP servers use the password entered when the user logs in to Cisco PAM.

Step 5 Click **Profiles** and select the user's Cisco PAM profiles. See Defining User Profiles for Desktop Application Access for more information.

Note Cisco PAM does not synchronize the LDAP profiles.

Step 6 Click **Save and Close**.

The following requirements (8.4, 8.5.5, 8.5.9–14) are all met through the use of LDAP as the authentication services:

- **PCI 8.4—***Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5—***Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9—***Change user passwords at least every 90 days.*
- **PCI 8.5.10—***Require a minimum password length of at least seven characters.*
- **PCI 8.5.11—***Use passwords containing both numeric and alphabetic characters.PCI Sub-Requirements with Compensating Controls*
- **PCI 8.5.12—***Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13—***Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14—***Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15—***If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco PAM has a hard-coded session timeout of 30 minutes in the configuration for the version validated. Administration time limits would need to be enabled systemically through an active directory policy to the admin workstation desktops, locking them when there is no activity after 15 minutes.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco PAM is able to track and monitor all administrative user access and events to meet the following requirements**:**

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*

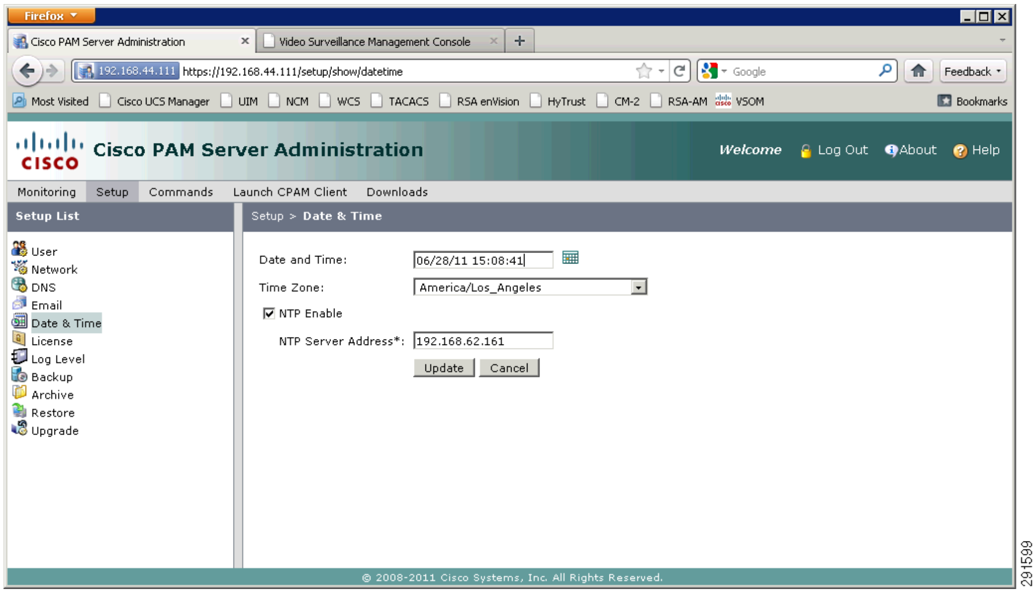
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco PAM and the gateways use the local clock facilities to meet the following requirements**:**

- **PCI 10.4.2—***Time data is protected.*
- **PCI 10.4.3—***Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. All the events in the Access Control system have a time stamp associated to them. Cisco PAM and the gateway are configured to use NTP, as shown in Figure 5-28.

Figure 5-28 Cisco PAM NTP Configuration


https://192.168.44.111/setup/show/datetime

Setup > Date & Time

Date and Time: 06/28/11 15:08:41

Time Zone: America/Los_Angeles

☑ NTP Enable

NTP Server Address*: 192.168.62.161

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects logging information from all devices to ensure the integrity and correlation of events.

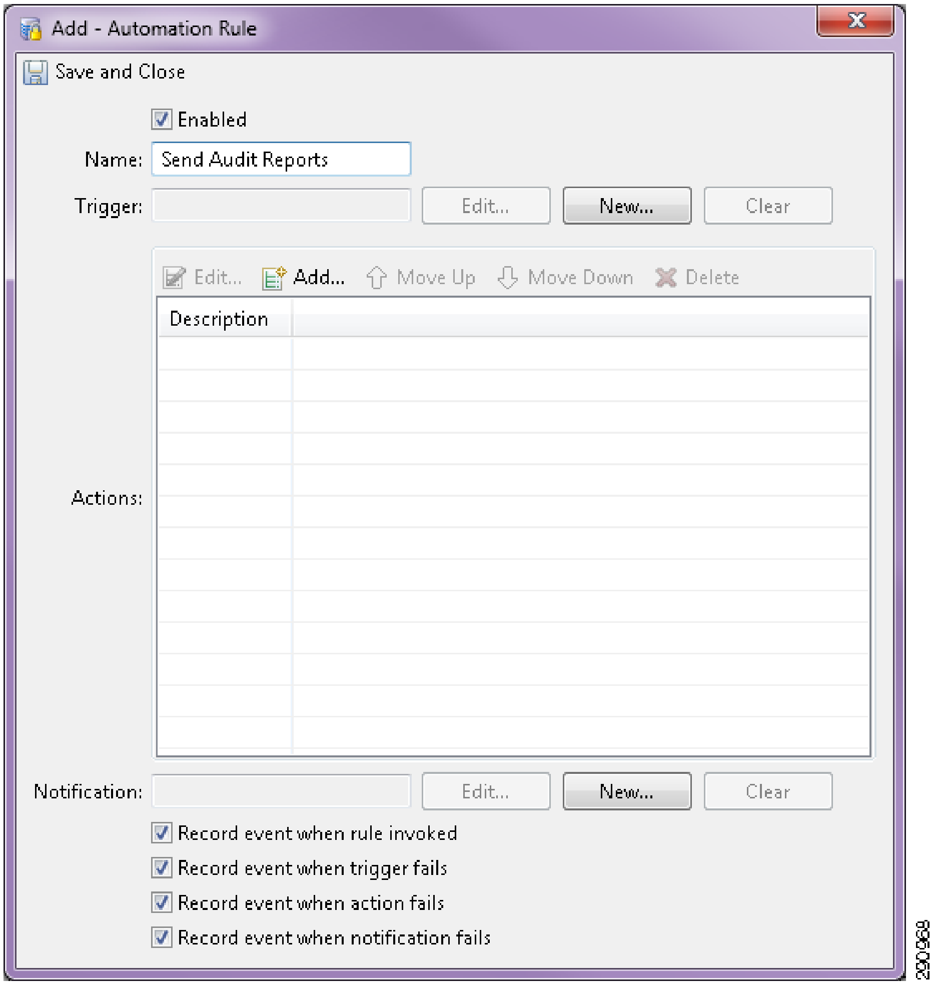
- **PCI 10.5—***Secure audit trails so they cannot be altered.*
- **PCI 10.5.1—***Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2—***Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3—***Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5—***Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco PAM allows for the creation of global I/O rules to trigger sending audit reports to a centralized server. Following are the instructions to create a global I/O with audit reports.

Step 1 In the Cisco PAM client, click **Events & Alarms -> Global I/O > Add**.

Step 2 Enter a name and click **New** in the Trigger field. (See Figure 5-29.)

Figure 5-29 Creating a Global I/O with Audit Reports



Add - Automation Rule

☑ Enabled

Name: Send Audit Reports

Trigger:

Actions:

Notification:

☑ Record event when rule invoked

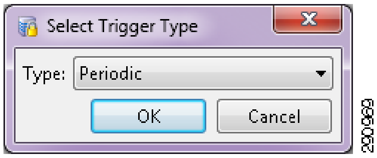
☑ Record event when trigger fails

☑ Record event when action fails

☑ Record event when notification fails

Step 3 Select **Periodic** and click **OK**. (See Figure 5-30.)

Figure 5-30 Selecting Periodic

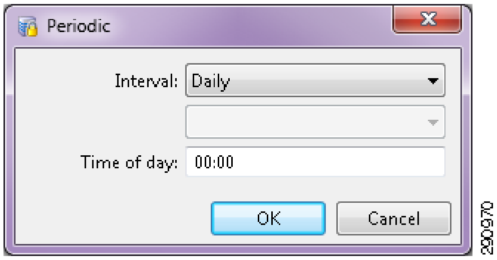


Select Trigger Type

Type: Periodic

Step 4 Choose the Interval and enter the Time of Day. Click **OK**. (See Figure 5-31.)

Figure 5-31 Selecting Interval and Time of Day



Periodic

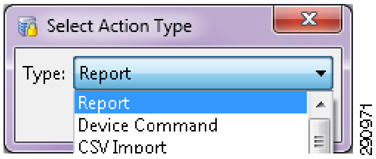
Interval: Daily

Time of day: 00:00

Step 5 Under Actions, Click **Add…**

Step 6 Select **Report.** (See Figure 5-32.)

Figure 5-32 Selecting Action Type

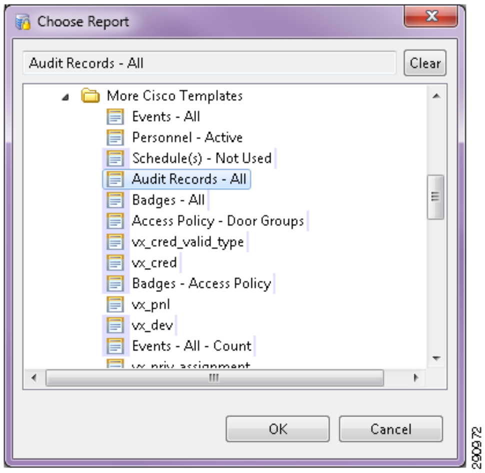


Select Action Type

Type: Report

Step 7 Choose **Audit Records–All** and click **OK**. (See Figure 5-33.)

Figure 5-33 Audit Records–All

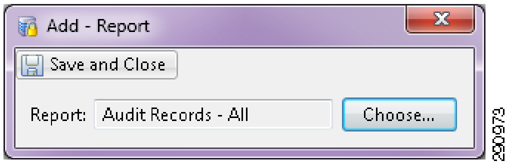


Choose Report

Audit Records - All

Step 8 Click **Save and Close**. (See Figure 5-34.)

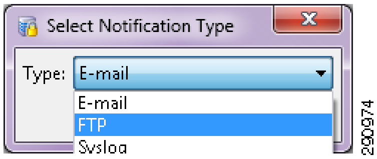
Figure 5-34 Save and Close



Report: Audit Records - All

Step 9 Under Notification section of the Global I/O, click **New** and Choose **FTP**. Click **OK**. (See Figure 5-35.)

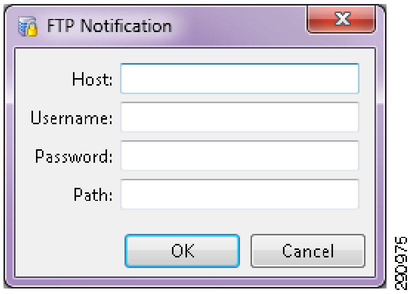
Figure 5-35 Select Notification Type



Type: E-mail

Step 10 Enter the FTP Host, Username, Password, and Path. Click **OK**. (See Figure 5-36.)

Figure 5-36 FTP Notification



Step 11 Click **Save and Close**. You should see a new entry created. You can create similar global I/O rules for every hour.

The audit report is read into RSA enVision server, which then maintains and protects the integrity of the file.

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

E-mail

Cisco IronPort Email Security Solution

Cisco IronPort Email Security Solution uses data loss prevention (DLP) technology to block e-mail that is inadvertently sent containing cardholder data information.

Note The Cisco IronPort Email Security Solution was initially reviewed by Verizon Business and determined to be outside the scope of the PCI Audit. There is no Assessment Summary or Capability Assessment details for this product. However, Cisco IronPort Email Security Solution could potentially store or transmit sensitive cardholder data if used with the default settings for message tracking. Sensitive information in messages would be automatically forwarded in clear text to administrators, and recipients. These same messages would also be stored un-encrypted. The design considerations below detail how to properly configure the Cisco IronPort Email Security Solution to avoid this pitfall.

Cisco IronPort Email Security Solution provides sophisticated and scalable mechanisms that help to minimize the downtime associated with e-mail-borne malware and simplify the administration of corporate e-mail systems, while offering insight into the e-mail system operation. Capabilities include the following:

- Spam protection
- Data loss prevention (DLP)
- Virus defense
- E-mail encryption tracking and reporting tools

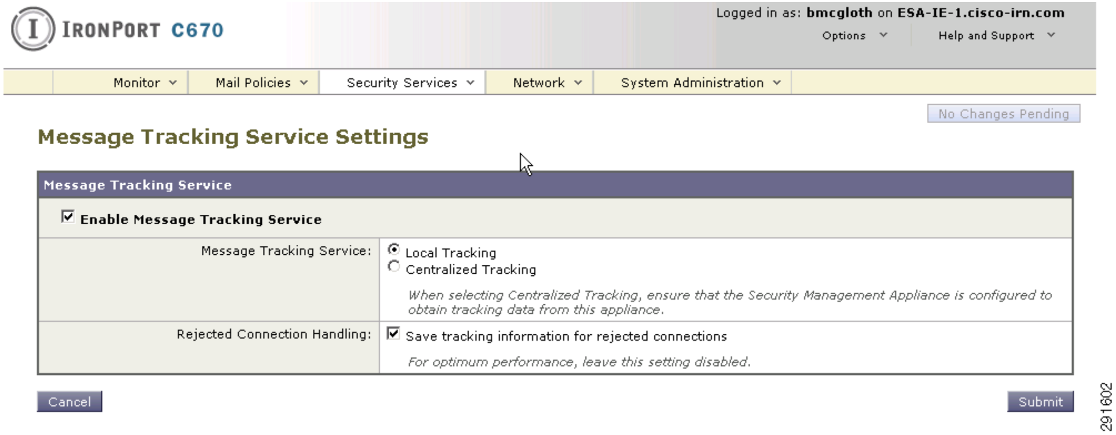
Primary PCI Function

Although data loss prevention is not covered by a specific PCI requirement, Cisco IronPort Email Security Solution helps in achieving PCI compliance by preventing the transmission of cardholder data over open public networks via e-mail.

Design Considerations

- Do not enable logging, storage, or forwarding messages identified as containing cardholder data.
- For IronPort to analyze messages passing through it, message tracking must be enabled, as shown in Figure 5-37.

Figure 5-37 Enable IronPort Message Tracking



Logged in as: **bmcgloth** on **ESA-IE-1.cisco-irn.com**

Message Tracking Service Settings

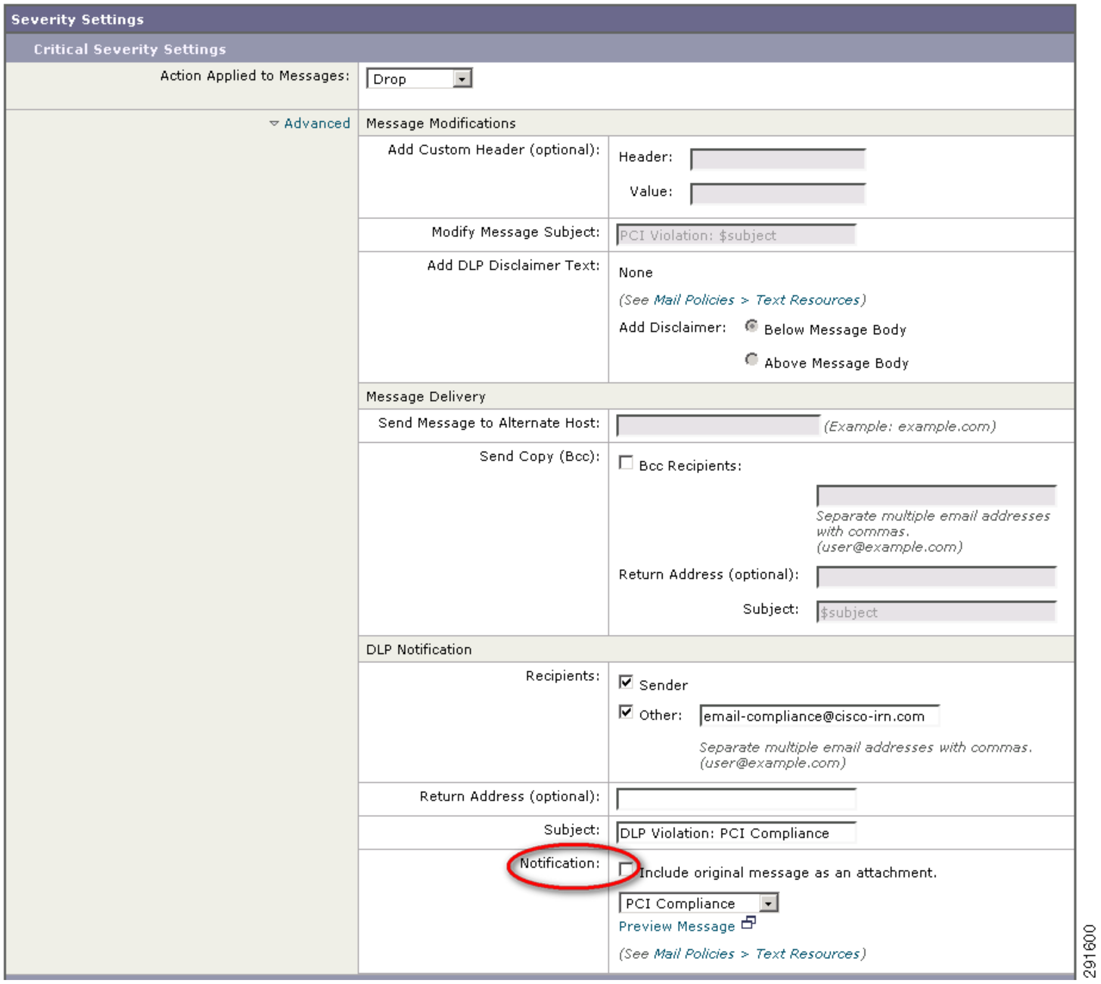
Message Tracking Service

☑ **Enable Message Tracking Service**

Message Tracking Service:	● Local Tracking ○ Centralized Tracking *When selecting Centralized Tracking, ensure that the Security Management Appliance is configured to obtain tracking data from this appliance.*
Rejected Connection Handling:	☑ Save tracking information for rejected connections *For optimum performance, leave this setting disabled.*

- Create policy in IronPort to drop messages containing credit card numbers, but not to forward that message to administrators. Ensure that the “include original message” checkbox is not selected, as shown in Figure 5-38.

Figure 5-38 Policy in IronPort Excluding Original Message



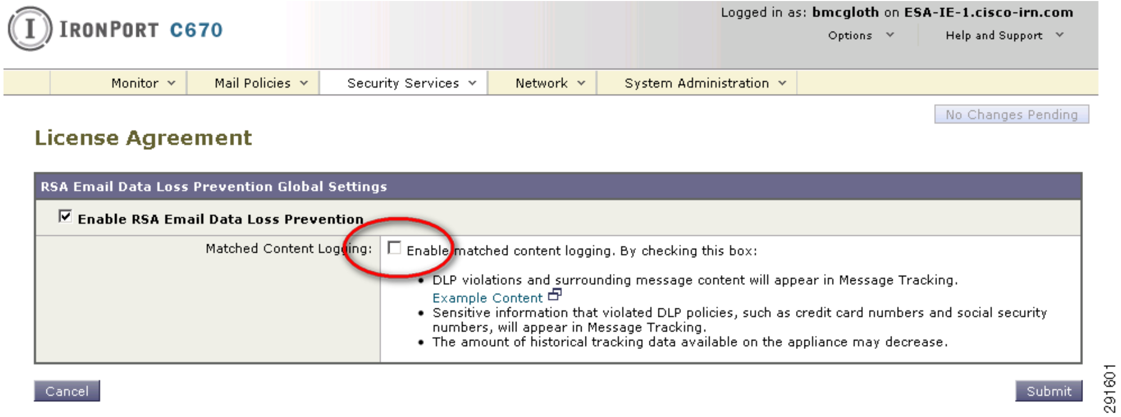
Severity Settings

Critical Severity Settings

Action Applied to Messages:	Drop	
▿ Advanced	Message Modifications	
	Add Custom Header (optional):	Header: Value:
	Modify Message Subject:	PCI Violation: $subject
	Add DLP Disclaimer Text:	None *(See Mail Policies > Text Resources)* Add Disclaimer: ● Below Message Body ○ Above Message Body
	Message Delivery	
	Send Message to Alternate Host:	*(Example: example.com)*
	Send Copy (Bcc):	□ Bcc Recipients: *Separate multiple email addresses with commas. (user@example.com)* Return Address (optional): Subject: $subject
	DLP Notification	
	Recipients:	☑ Sender ☑ Other: email-compliance@cisco-irn.com *Separate multiple email addresses with commas. (user@example.com)*
	Return Address (optional):	
	Subject:	DLP Violation: PCI Compliance
	Notification:	□ Include original message as an attachment. PCI Compliance Preview Message *(See Mail Policies > Text Resources)*

- To ensure that messages identified as containing credit card information are not stored in the local system, you must disable logging of matched content, as shown in Figure 5-39. The local log of the IronPort server is not a safe encrypted place to store cardholder data.

Figure 5-39 IronPort DLP—Matched Content Logging Disabled



License Agreement

RSA Email Data Loss Prevention Global Settings

☑ Enable RSA Email Data Loss Prevention

Matched Content Logging: □ Enable matched content logging. By checking this box:

- DLP violations and surrounding message content will appear in Message Tracking. Example Content
- Sensitive information that violated DLP policies, such as credit card numbers and social security numbers, will appear in Message Tracking.
- The amount of historical tracking data available on the appliance may decrease.

Hosts

Cisco Unified Computing System

The Cisco Unified Computing System (UCS) is used to securely deploy sensitive and compliance-related applications. Provisioning options, including virtualization technology, allow the mixing of sensitive and non-sensitive applications without compromising scope boundaries.

Improve IT responsiveness to rapidly changing business demands with this next-generation data center platform. Cisco UCS accelerates the delivery of new services simply, reliably, and securely through end-to-end provisioning and migration support.

Benefits include the following:

- Streamlines data center resources to reduce total cost of ownership
- Scales service delivery to increase business agility
- Radically reduces the number of devices requiring setup, management, power, cooling, and cabling

Table 5-14 PCI Assessment Summary—Cisco UCS

Models Assessed	
Cisco UCS Manager version 1.3(1p)	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15

Table 5-14 PCI Assessment Summary—Cisco UCS (continued)

PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of Cisco UCS is to securely host one primary compliance-related function per physical or virtual server.

It provides segmentation of sensitive applications from out-of-scope applications via physical and virtualization technology. Although technically, a firewall or ACL is used to enforce PCI Requirement 1, Cisco UCS extends Layer 3 boundaries to virtual network and storage adapters within the chassis. Using VLANs and VSANs, Cisco UCS allows a retailer to separate its payment systems (in-scope) from other non-sensitive data (out-of-scope).

Table 5-14 lists the component assessment details for Cisco UCS.

Table 5-15 Component Capability Assessment—Cisco Unified Computing System

Cisco Unified Computing System	
PRIMARY FUNCTION	Requirement N/A
Securely host payment applications.	
CAPABILITY	ASSESSMENT
Secure Services	
Disabled any unnecessary services—*“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- Cisco UCS allows for the provisioning of individual servers on blades. Each blade can host a native operating system such as Windows 2008 server, or a virtualization hypervisor system such as VMware ESX/ESXi. These provisioning options represent a primary function for the server blade. In the lab validation, VMware ESX was installed on each of the Cisco UCS blades, and several VM hosts were then configured, each with one primary function. Each server blade is provisioned via a profile. Profiles can be created locally in Cisco UCS Manager or centrally using the Vblock provisioning utility, Unified Infrastructure Manager (UIM), which provides simplified Vblock management by combining provisioning with configuration, change, and compliance management.
- EMC SAN is a primary component of the VCE architecture for Vblock Infrastructure Platforms. Vblock 1 is designed for medium to high numbers of virtual machines, and is ideally suited to a broad range of usage scenarios, including shared services, e-mail, file and print, virtual desktops, and collaboration.
- Cisco UCS allows for the provisioning of individual servers on blades. Each blade can host a native operating system such as Windows 2008 server, or a virtualization hypervisor system such as VMware ESX/ESXi.
- Each Cisco UCS server blade is provisioned via a profile. Profiles can be created locally in Cisco UCS Manager or centrally using the Vblock provisioning utility, EMC Unified Infrastructure Manager (UIM), which provides simplified Vblock management by combining provisioning with configuration, change, and compliance management.
- The PCI standard requires one primary function per server. When using virtualization technology, the single primary server function is extended to individual virtual machines.
- The hypervisor of an individual blade is considered insecure for segmenting scopes of compliance. Therefore, when putting non-sensitive VM servers with sensitive VM servers on the same physical blade, the non-sensitive would be included in the scope of the audit.
- The UCS system securely segments network and storage to each blade, which allows mixing of sensitive and non-sensitive applications across different physical blades of the chassis.
- PCI requires a 15-minute timeout for administrative functions. Cisco UCS does not feature an explicit session timeout. Administration time limits would need to be enabled systemically through active directory policy to the admin workstation desktops, locking them when there is no activity.

  Cisco UCS was implemented using the Cisco UCS installation guides: http://www.cisco.com/en/US/products/ps10276/prod_installation_guides_list.html

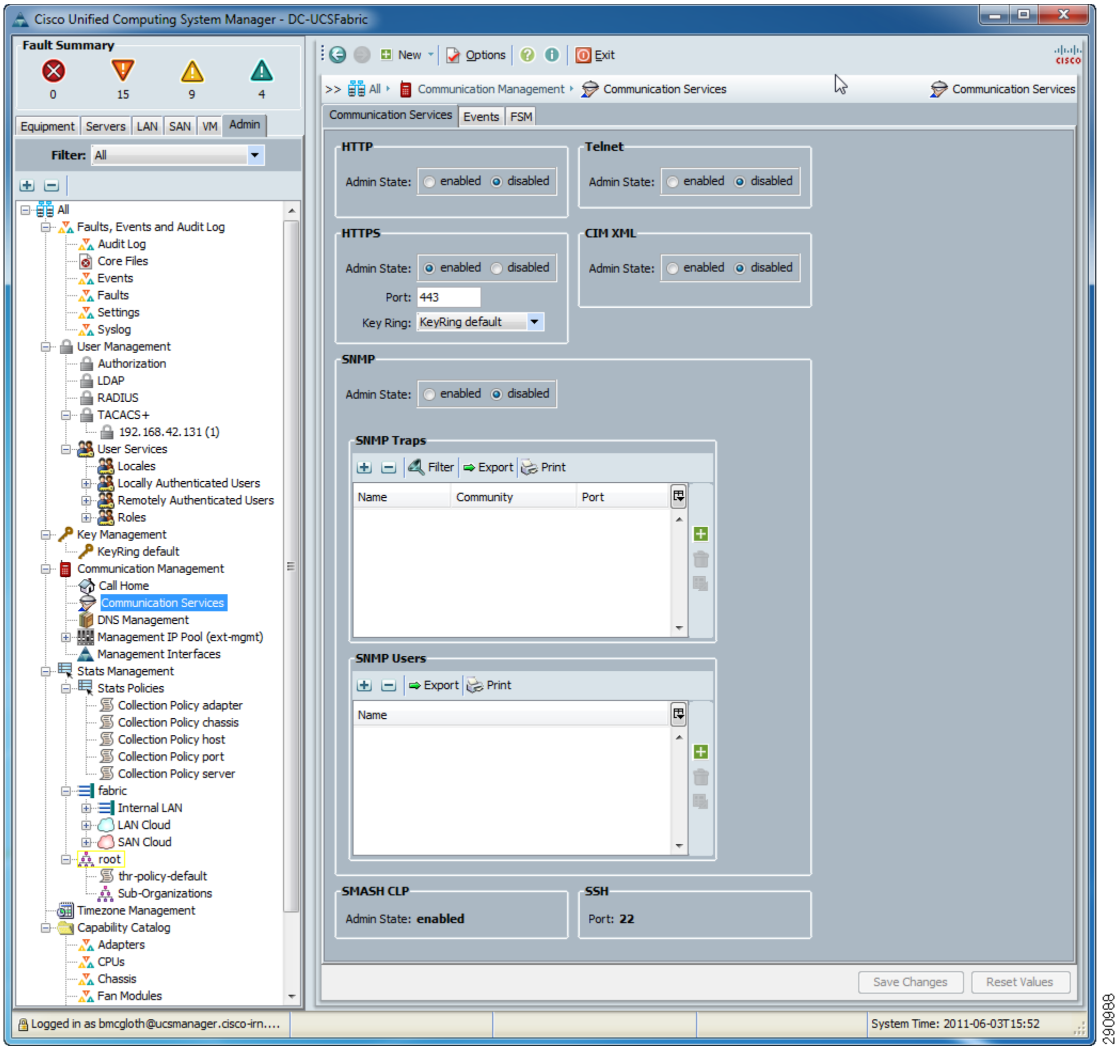
PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco UCS allows for the disabling of non-secure administrative interfaces. Figure 5-40 shows the secure management protocols of SSH and HTTPS for administration. Telnet, HTTP, and other unused protocols are disabled.

Figure 5-40 Secure Management Protocols



Cisco Unified Computing System Manager - DC-UCSFabric

Fault Summary: 0, 15, 9, 4

Filter: All

>> All ▸ Communication Management ▸ Communication Services

Communication Services | Events | FSM

HTTP
Admin State: ○ enabled ● disabled

Telnet
Admin State: ○ enabled ● disabled

HTTPS
Admin State: ● enabled ○ disabled
Port: 443
Key Ring: KeyRing default

CIM XML
Admin State: ○ enabled ● disabled

SNMP
Admin State: ○ enabled ● disabled

SNMP Traps

Name	Community	Port

SNMP Users

Name

SMASH CLP
Admin State: enabled

SSH
Port: 22

Logged in as bmcgloth@ucsmanager.cisco-irn....

System Time: 2011-06-03T15:52

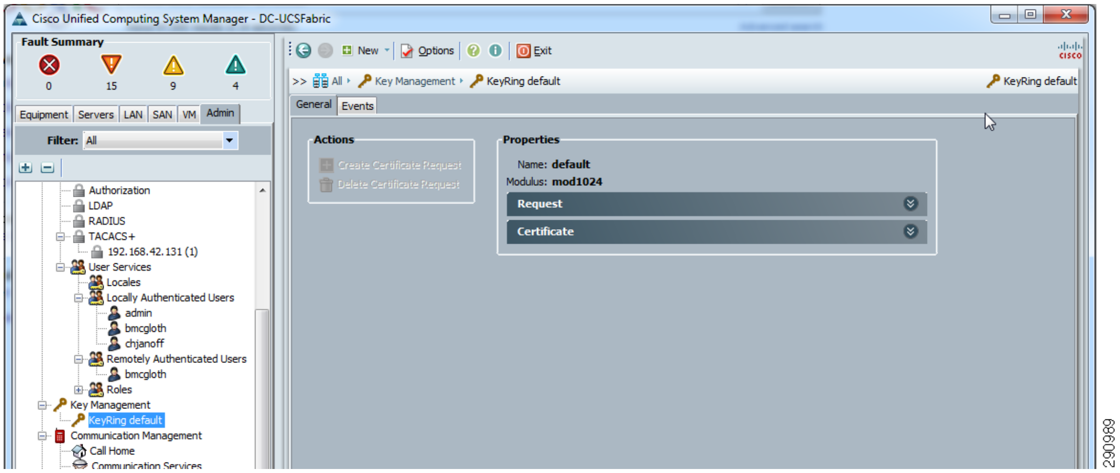
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco UCS does not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco UCS uses strong encryption for SSH and HTTPS connections. Encryption keys are created and managed under the Key Management feature. (See Figure 5-41.)

Figure 5-41 1024-Bit Mod Key Default Keyring



Name: default
Modulus: mod1024

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco UCS. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

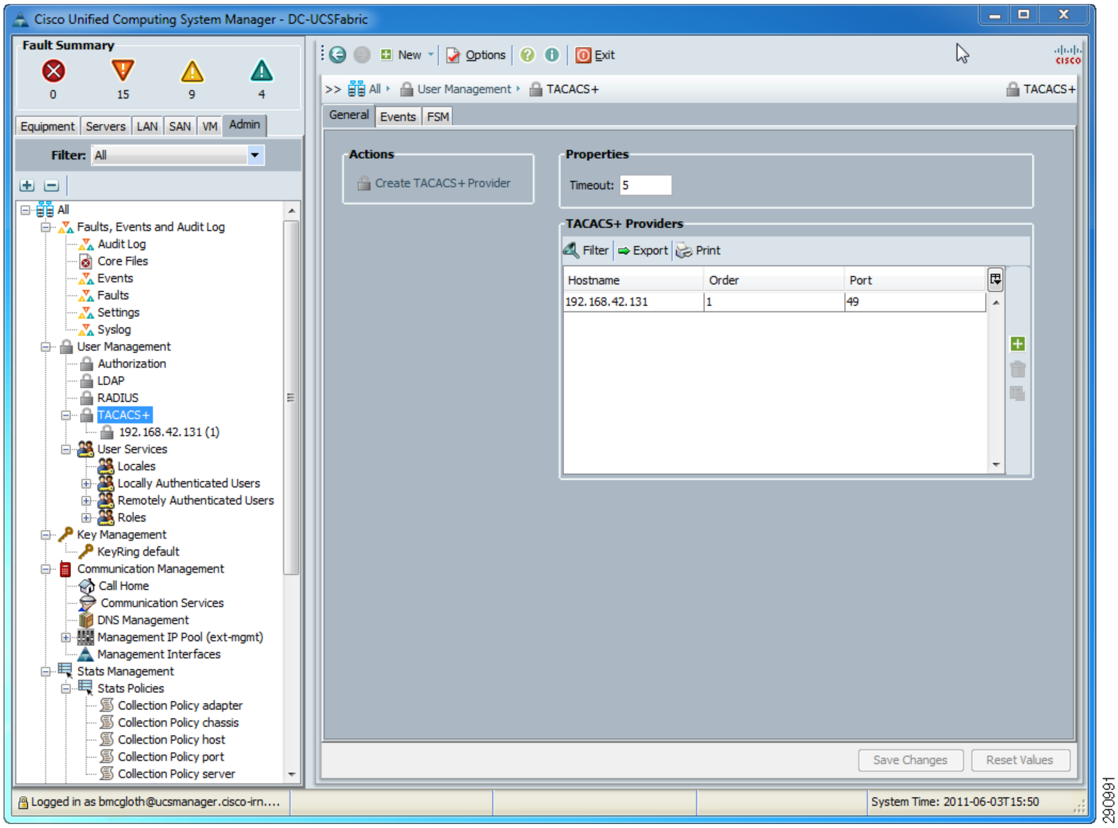
The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*

- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Add the Cisco Secure ACS server under the TACACS+ protocol option, as shown in Figure 5-42.

Figure 5-42 Adding the Cisco Secure ACS Server



Timeout: 5

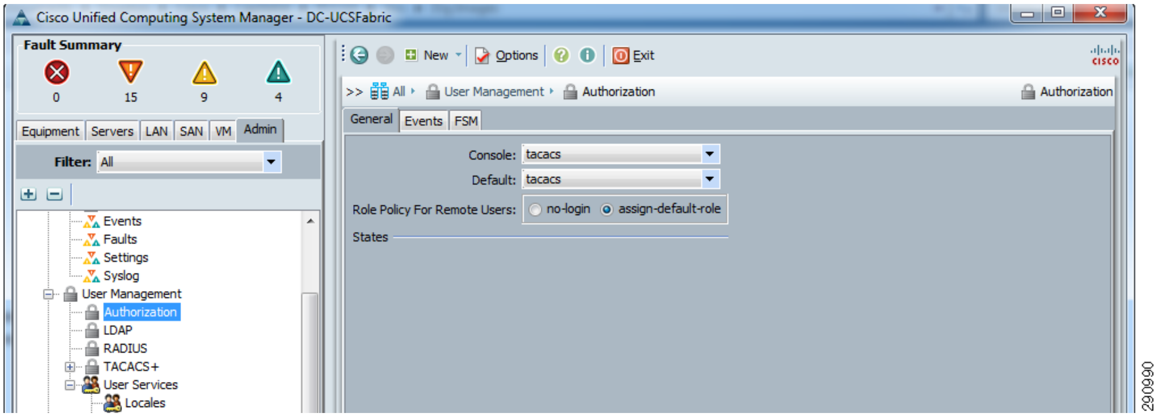
Hostname	Order	Port
192.168.42.131	1	49

Logged in as bmcgloth@ucsmanager.cisco-irn....

System Time: 2011-06-03T15:50

Select **tacacs** from the Console and Default dropdown menus on the Authorization page, as shown in Figure 5-43.

Figure 5-43 Authorization—Selecting Console and Default Settings



Console: tacacs

Default: tacacs

Role Policy For Remote Users: ○ no-login ● assign-default-role

On the TACACS+ server, create custom attributes defining the desired role for the user or group accessing the Cisco UCS Manager (see Figure 5-44):

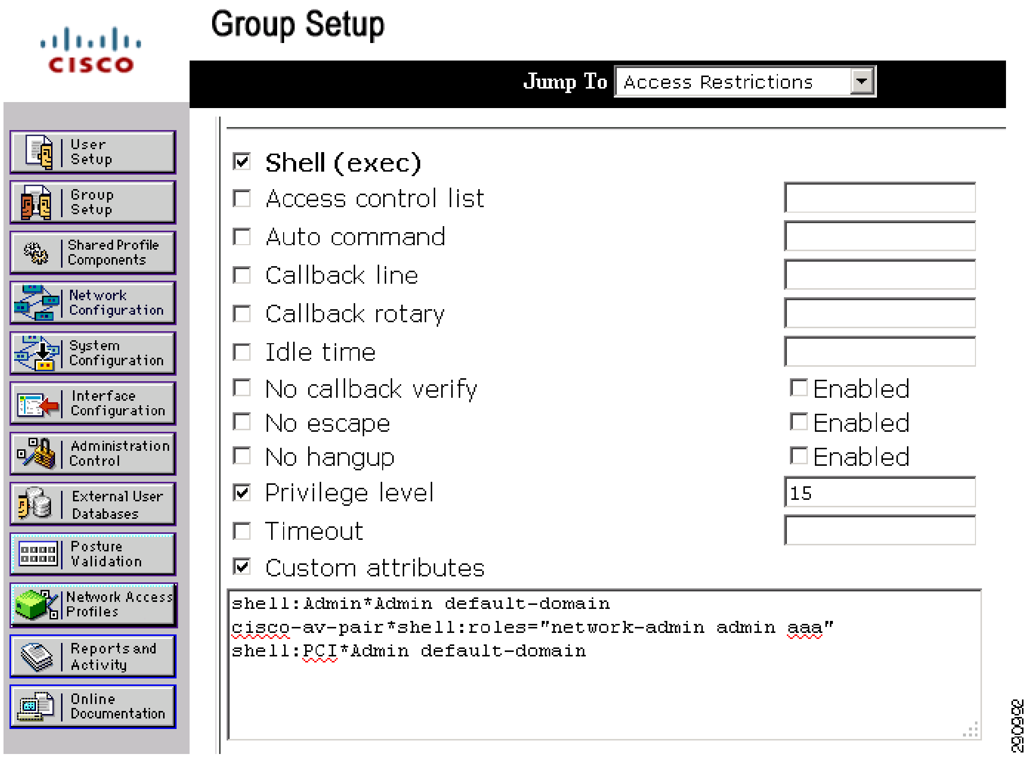
- TACACS+ custom attributes for UCS Manager:

```
cisco-av-pair*shell:roles="admin aaa"
```

- If combined with other systems roles, such as for the Nexus;

```
cisco-av-pair*shell:roles="network-admin admin aaa"
```

Figure 5-44 Group Configuration Page on TACACS+ Server



Group Setup

Jump To: Access Restrictions

☑ Shell (exec)
□ Access control list
□ Auto command
□ Callback line
□ Callback rotary
□ Idle time
□ No callback verify □ Enabled
□ No escape □ Enabled
□ No hangup □ Enabled
☑ Privilege level 15
□ Timeout
☑ Custom attributes

```
shell:Admin*Admin default-domain
cisco-av-pair*shell:roles="network-admin admin aaa"
shell:PCI*Admin default-domain
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

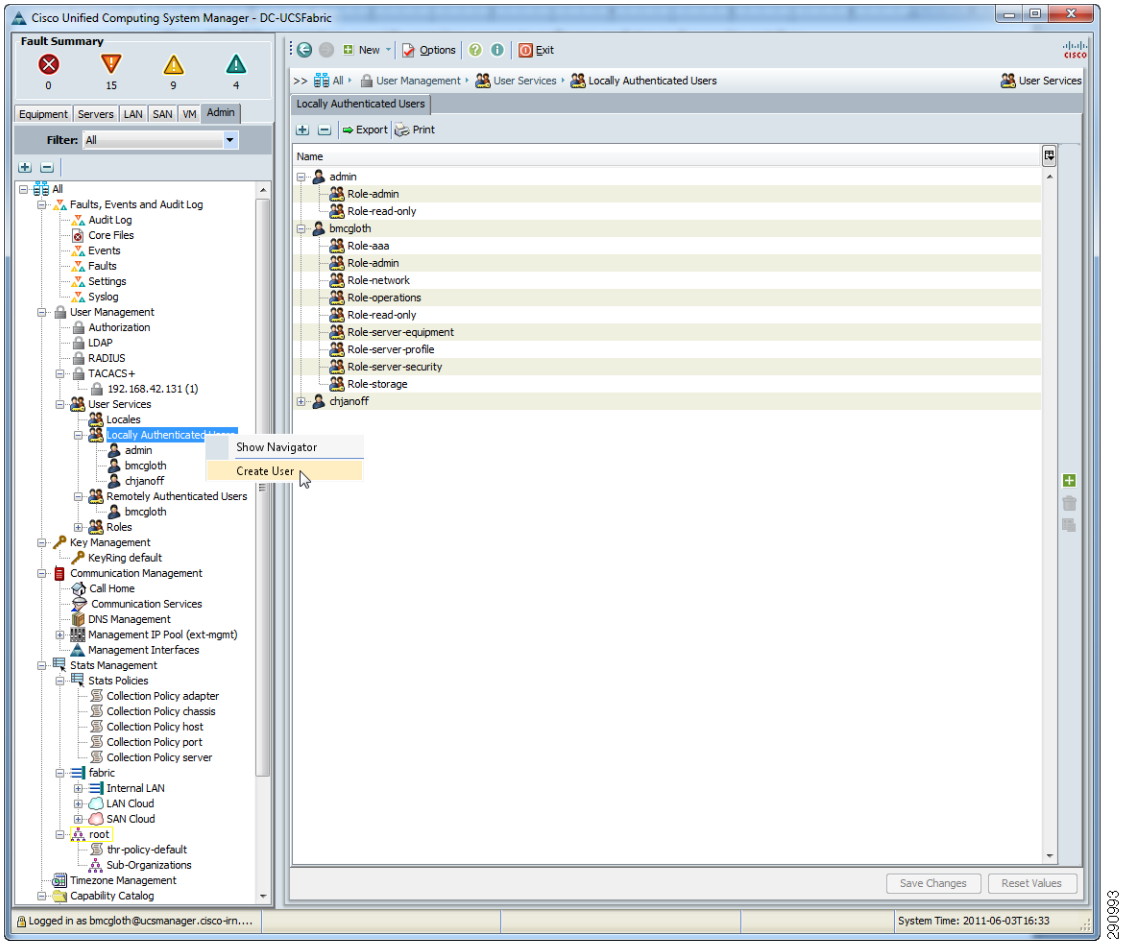
Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown above in Requirement 7.

The Cisco UCS is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco UCS supports the creation of local user accounts with unique IDs through the use of the Create User option when you alt-click on Locally Authenticated Users (see Figure 5-45). These can be used for local fallback user accounts.

Figure 5-45 Create User



- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco UCS require setting of a password for admin role accounts.
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Local passwords are stored encrypted on the Cisco UCS system and are not displayed.
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco UCS servers allow for an administrator to specify an expiration date for the local user accounts passwords, effectively disabling their accounts after a specified period of time.
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco UCS does not support an automated capability to perform this function at this time; user passwords management would have to be manually performed every 90 days per a company policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco UCS servers require a minimum of eight characters for local passwords.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters. PCI Sub-Requirements with Compensating Controls*

  Cisco UCS servers require at least three of the following character types for passwords:

  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco UCS does not support an automated capability to perform this function at this time; user account management would have to follow this policy manually if a centralized authentication service with this capability could not be used.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco UCS does not support the ability to lock out local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco UCS does not support the ability to lock out local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco UCS does not feature an explicit session timeout. Administration time limits would need to be enabled systemically through an Active Directory policy to the admin workstation desktops, locking them when there is no activity after 15 minutes.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco UCS is able to track and monitor all administrative user access, events such as profile creation, interface up/down, and device authentications.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*

  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco UCS is able to track and monitor all administrative user access and events.

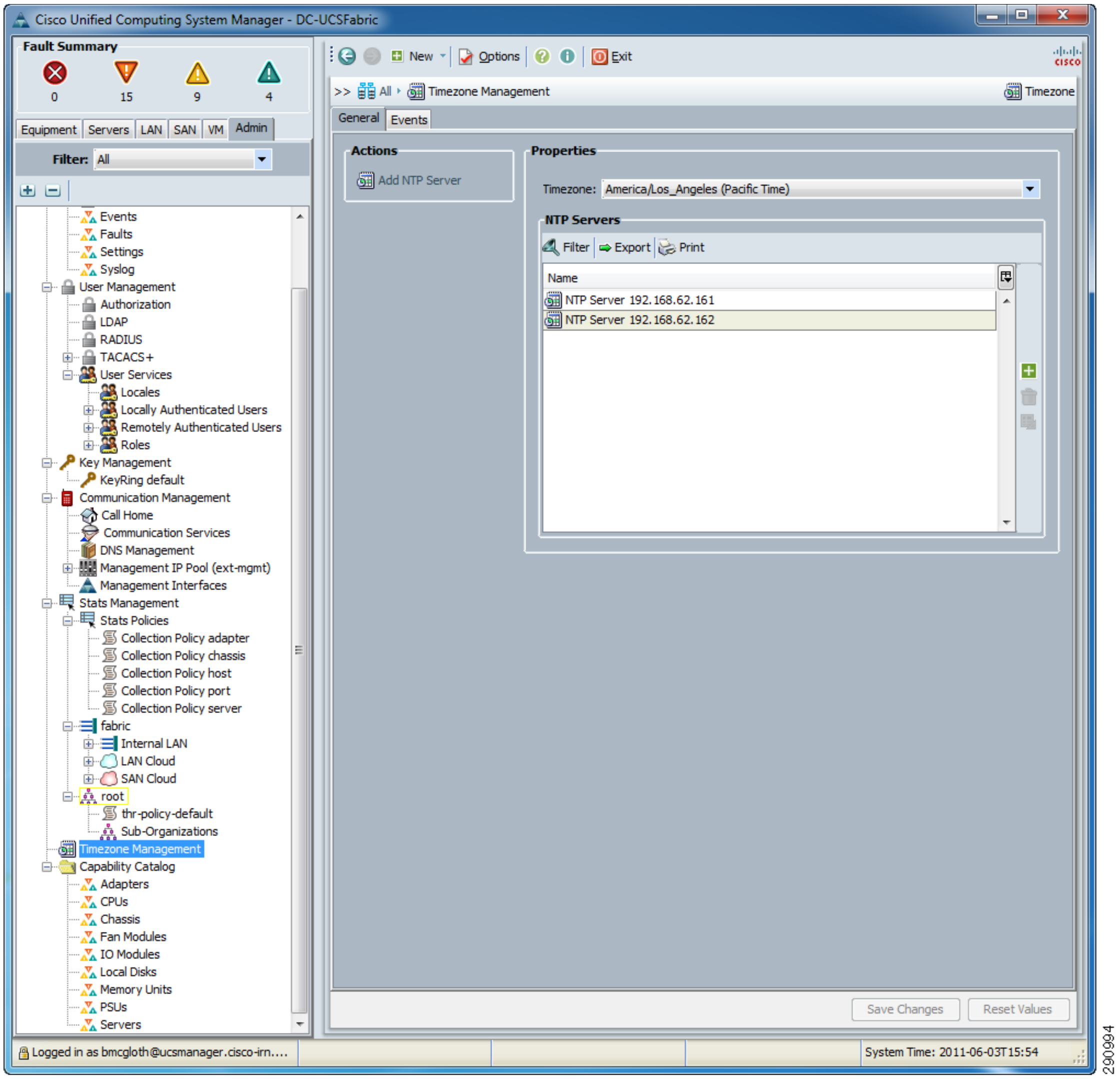
- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco UCS uses NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices (see Figure 5-46). This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

Figure 5-46 NTP Screen



Timezone: America/Los_Angeles (Pacific Time)

NTP Server 192.168.62.161
NTP Server 192.168.62.162

Logged in as bmcgloth@ucsmanager.cisco-irn....

System Time: 2011-06-03T15:54

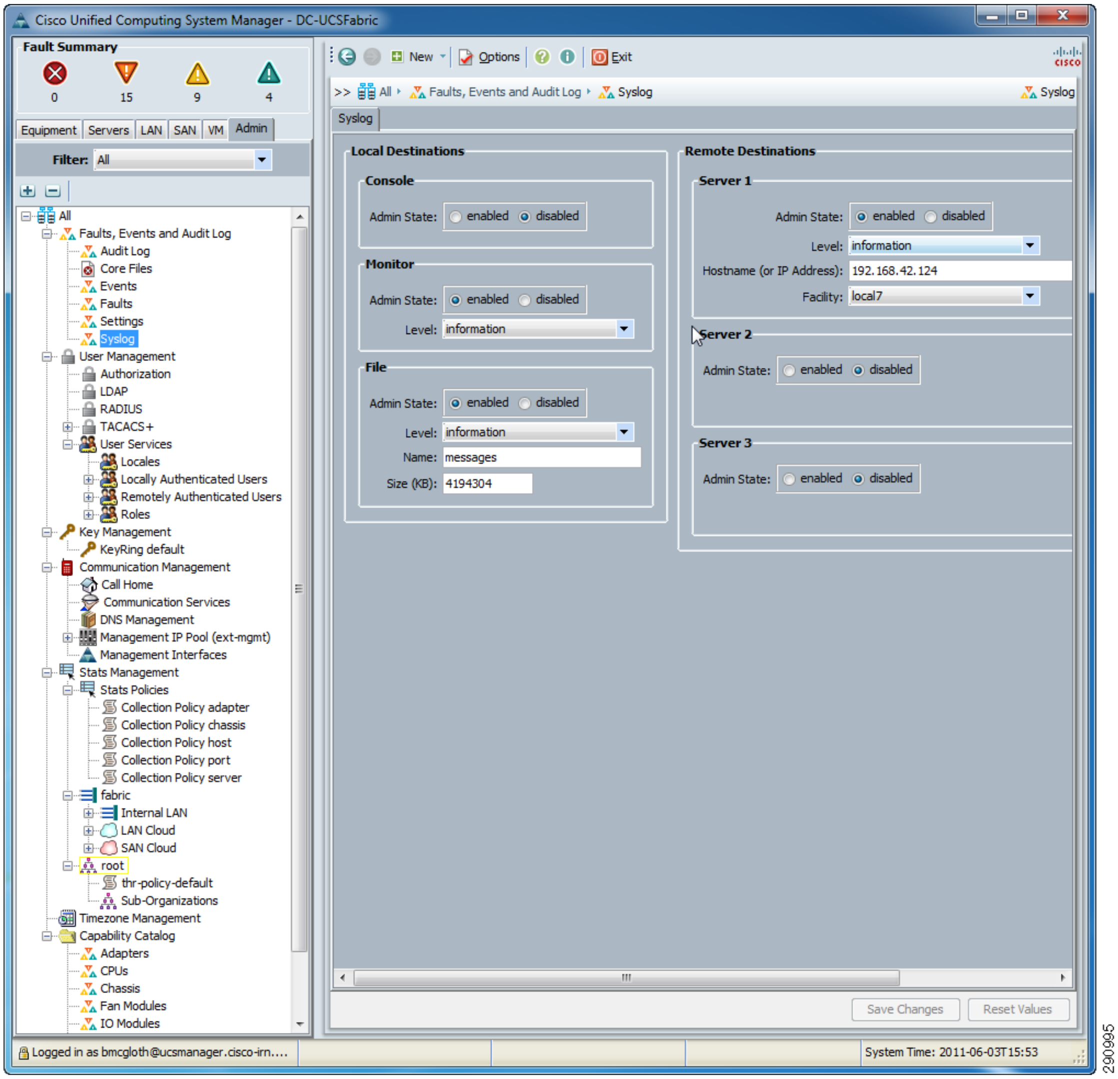
To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Requirement 10.5 was met using RSA enVision, which is a central logging repository that collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

Cisco UCS is capable of sending system events to a centralized repository using the syslog function and/or SNMP traps. In the solution, only syslog was used. (See Figure 5-47.)

Figure 5-47 Using Syslog



Local Destinations

Console

Admin State: ○ enabled ● disabled

Monitor

Admin State: ● enabled ○ disabled

Level: information

File

Admin State: ● enabled ○ disabled

Level: information

Name: messages

Size (KB): 4194304

Remote Destinations

Server 1

Admin State: ● enabled ○ disabled

Level: information

Hostname (or IP Address): 192.168.42.124

Facility: local7

Server 2

Admin State: ○ enabled ● disabled

Server 3

Admin State: ○ enabled ● disabled

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco UCS Express on Services Ready Engine

The Cisco Unified Computing System Express (UCS Express) and Services Ready Engine (SRE) allows retailers to securely deploy sensitive applications directly within the routing platform. By using UCS Express, retailers can remove legacy compute resources in the store, saving space, energy, and operational costs.

Cisco UCS Express is a converged networking, computing, and virtualization platform for hosting essential business applications in the store location. The SRE modules are router blades for the second generation of Cisco Integrated Services Routers (ISR G2) that provide the capability to host Cisco, third-party, and custom applications. A service-ready deployment model enables store applications to be provisioned remotely on the modules at any time. Cisco SRE modules have their own processors, storage, network interfaces, and memory, which operate independently of the host router resources and help ensure maximum concurrent routing and application performance.

Table 5-16 PCI Assessment Summary—Cisco UCS Express and Cisco SRE

Models Assessed	
Cisco UCS Express version 1.1 on SRE900	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
PCI 8	8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of Cisco UCS Express is to securely host one primary compliance-related function per physical or virtual server.

It provides segmentation of sensitive applications from out-of-scope applications via physical and virtualization technology. Although technically, a firewall or ACL is used to enforce PCI Requirement 1, UCS extends Layer 3 boundaries to virtual NIC and storage adapters within the chassis. Using VLANs and VSANs, Cisco UCS allows a retailer to separate its payment systems (in-scope) from other non-sensitive data (out-of-scope).

Table 5-16 lists the component assessment details for the Cisco UCS Express and Cisco SRE.

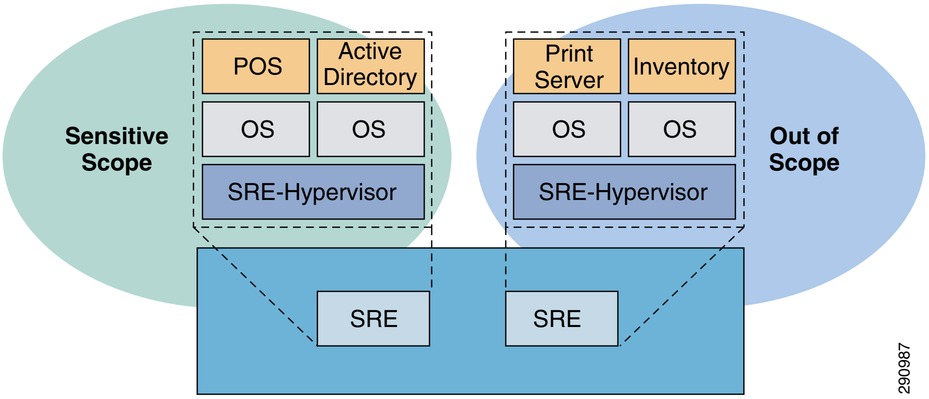
Table 5-17 Component Capability Assessment—Cisco UCS Express and Cisco SRE

Cisco UCS Express and Cisco SRE	
PRIMARY FUNCTION	**Requirement N/A**
Securely host payment applications.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	🟢
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	🟢
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	🟢
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	▽
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	🟢

Design Considerations

The major consideration when using Cisco UCS Express with sensitive applications is the security of the hypervisor. PCI considers all hypervisors to be insecure. Therefore, use separate Cisco UCS Express implementations when scooping. Although it is acceptable to mix non-sensitive applications onto a Cisco UCS Express deployment with sensitive applications, that brings those applications into scope and audit. (See Figure 5-48.)

Figure 5-48 Using UCS Express with Cisco SRE



- The audited version 1.1 of UCS Express has several limitations with local user accounts. There is no capability to use central authentication or management. This resulted in a need for compensating controls that are detailed below.

Note Newer versions of UCS Express (version 1.5 +) enable central management of the VMware ESXi on Cisco UCS Express through vCenter (upgrade license required) as well as eliminate the Cisco console VM and local user management/VMware ESXi management restrictions. With the new release, Cisco UCS can manage users on VMware ESXi exactly as it would on a standalone VMware ESXi 4.1 server. This feature was not able to be validated before publishing of this guide, and has not been assessed by Verizon Business or tested in the Cisco PCI solution lab.

Note The Cisco UCS Express module comes installed with VMware ESXi. This is the primary function for the server module. Each module can host several independent operating systems as virtual servers. Each virtual server should have only one primary function.

- Cisco UCS Express requires the use of VLANs in the router. Depending on the deployment within the store, this may require the use of bridged virtual interfaces.
- Cisco UCS Express is based on VMware's ESXi and uses vSphere client for management.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco UCS Express and the underlying VMware ESXi have no unnecessary services enabled by default.
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco UCS Express appliance does not allow changes to the operating system, installation of unsupported hardware, or of unsupported third-party software.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco UCS Express uses strong encryption for SSH and HTTPS connections.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for* *example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco UCS Express. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the internal database for administrator users. Individual administrative user IDs are created and assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco UCS Express includes extensive controls for defining user privileges and by default denies access to all individuals without a system user ID.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco UCS Express supports the creation of local user accounts with unique IDs through the use of the VMware vSphere client editing the local users and groups database.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco UCS Express require setting of a password.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  All passwords are stored using strong encryption.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Administrative time limits would need to be enabled systemically through an active directory policy to the admin workstation desktops, locking them when there is no activity.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco UCS Express is able to track and monitor all administrative user access, events such as profile creation, interface up/down, and device authentications.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

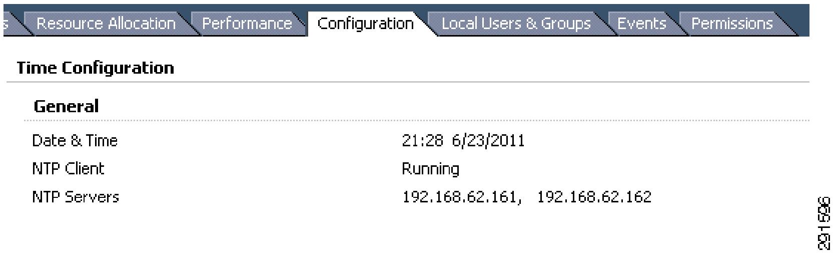
Cisco UCS Express uses the local clock facilities to meet the following requirements:

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*

  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers, as shown in Figure 5-49.

Figure 5-49 UCS Express NTP Servers



Time Configuration

General

Date & Time 21:28 6/23/2011

NTP Client Running

NTP Servers 192.168.62.161, 192.168.62.162

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

PCI Assessment Detail—PCI Sub-Requirements with Compensating Controls

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved using policies implemented through manual administration.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

Note Newer versions of UCS Express (version 1.5 +) enable central management of the VMware ESXi on UCS Express through vCenter (upgrade license required) as well as eliminate the Cisco console VM and local user management/VMware ESXi management restrictions. With the new release, Cisco UCS can manage users on VMware ESXi exactly as it would on a standalone VMware ESXi 4.1 server. This feature was not able to be validated before publishing of this guide, and has not been assessed by Verizon Business or tested in the Cisco PCI solution lab.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Scope Administration

Authentication

Cisco Secure Access Control Server

Cisco Secure Access Control Server (ACS) was used as a central authentication system for the majority of products validated in this solution. It links user authentication to Windows Active Directory using group mapping that segments users based on their role and function.

Cisco Secure ACS is an access policy control platform that helps you comply with growing regulatory and corporate requirements. By using a single authentication method for all system devices, insight into who made changes is simplified for internal administration, assessors, and post-breach audits. It supports multiple scenarios simultaneously, including the following:

- Device administration—Authenticates administrators, authorizes commands, and provides an audit trail
- Remote access—Works with VPN and other remote network access devices to enforce access policies
- Wireless—Authenticates and authorizes wireless users and hosts and enforces wireless-specific policies
- Network admission control—Communicates with posture and audit servers to enforce admission control policies

Cisco Secure ACS lets you centrally manage access to network resources for a growing variety of access types, devices, and user groups. These key features address the current complexities of network access control:

- Support for a range of protocols including Extensible Authentication Protocol (EAP) and non-EAP protocols provides the flexibility to meet all your authentication requirements

- Integration with Cisco products for device administration access control allows for centralized control and auditing of administrative actions
- Support for external databases, posture brokers, and audit servers centralizes access policy control and lets you integrate identity and access control systems

Table 5-18 PCI Assessment Summary—Cisco Secure Access Control Server

Models Assessed	
Cisco Secure Access Control Server	Release 4.2(1) Build 15 Patch 3
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of Cisco Secure ACS is to securely authenticate users toi the systems within the cardholder environment.

Table 5-18 lists the component assessment details for Cisco Secure ACS.

Table 5-19 Component Capability Assessment—Cisco Secure ACS

Cisco Secure ACS	
PRIMARY FUNCTION	**Requirement 7, 8 (7.1, 7.2, 8.2)**
Securely authenticate users to systems in the cardholder environment.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- Cisco Secure ACS has been configured to authenticate individual users using Active Directory (AD). This is accomplished by creating user groups in AD and mapping them to role-based groups in Cisco Secure ACS. This provides the granularity of secure authentication needed to address the PCI specification.
- The solution used the windows versions of Cisco Secure ACS. The CSA client was installed to protect and alert on unauthorized access of the log and audit trail.
- Remove the default accounts for administration.
- Enable HTTPS and disable HTTP.
- User authentication services for Cisco Secure ACS are linked to a centralized Active Directory user database

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*

If Cisco Secure ACS is deployed on a server, it should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

If Cisco Secure ACS is deployed as an appliance, no unnecessary services are enabled by default.

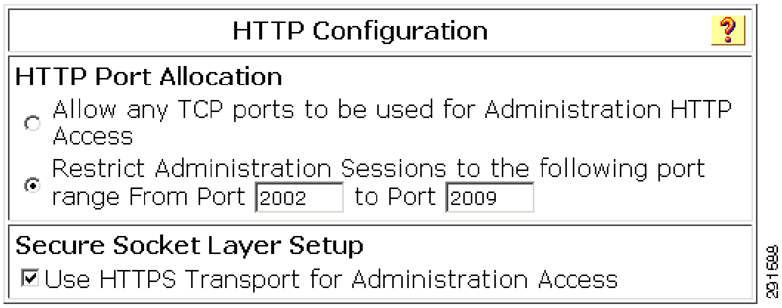
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Secure ACS should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

  If Cisco Secure ACS is deployed as an appliance, no unnecessary services are enabled by default.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The management console was configured to support HTTPS access, with HTTP access disabled. Cisco Secure ACS is configured to use SSL as a highly secure management portal technology (see Figure 5-50). Cisco Secure ACS employs port hopping to a random high port for secured communication transport.

Figure 5-50 HTTP Configuration



HTTP Configuration

HTTP Port Allocation

○ Allow any TCP ports to be used for Administration HTTP Access

● Restrict Administration Sessions to the following port range From Port 2002 to Port 2009

Secure Socket Layer Setup

☑ Use HTTPS Transport for Administration Access

Note Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant/service provider.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Secure ACS. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the Cisco Secure ACS internal database for administrator users. Within Cisco Secure ACS, individual administrative user IDs were created and assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco Secure ACS includes extensive controls for defining user privileges and by default denies access to all individuals without a system User ID.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database as shown below.

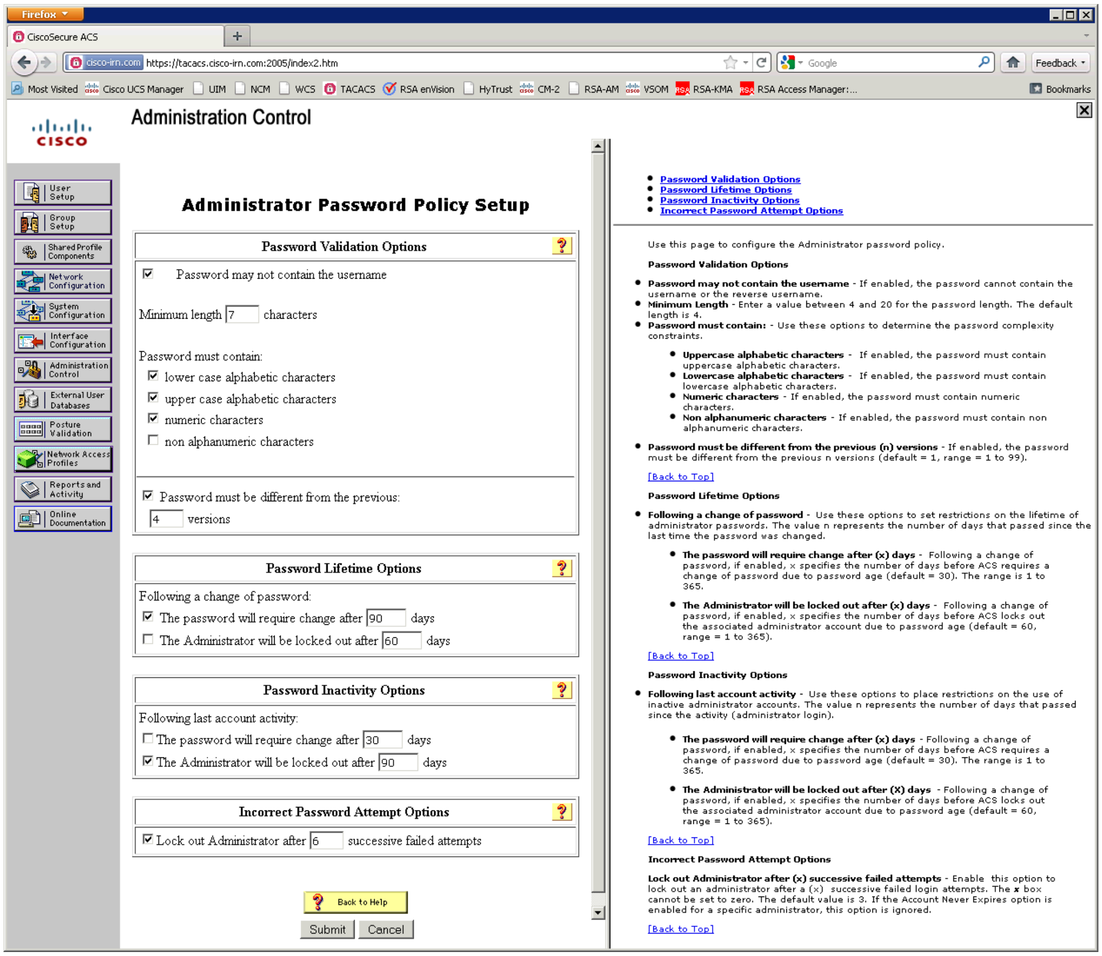
- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco Secure ACS supports the creation of local users. Through company policy, each user must be assigned a unique ID.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local administrator user accounts in Cisco Secure ACS require setting of a password according to the password requirements, as shown in Figure 5-51.

Figure 5-51 Administrator Password Requirements



Administrator Password Policy Setup

Password Validation Options

☑ Password may not contain the username

Minimum length 7 characters

Password must contain:

☑ lower case alphabetic characters

☑ upper case alphabetic characters

☑ numeric characters

☐ non alphanumeric characters

☑ Password must be different from the previous:
4 versions

Password Lifetime Options

Following a change of password:

☑ The password will require change after 90 days

☐ The Administrator will be locked out after 60 days

Password Inactivity Options

Following last account activity:

☐ The password will require change after 30 days

☑ The Administrator will be locked out after 90 days

Incorrect Password Attempt Options

☑ Lock out Administrator after 6 successive failed attempts

- Password Validation Options
- Password Lifetime Options
- Password Inactivity Options
- Incorrect Password Attempt Options

Use this page to configure the Administrator password policy.

Password Validation Options

- **Password may not contain the username** - If enabled, the password cannot contain the username or the reverse username.
- **Minimum Length** - Enter a value between 4 and 20 for the password length. The default length is 4.
- **Password must contain:** - Use these options to determine the password complexity constraints.
    - **Uppercase alphabetic characters** - If enabled, the password must contain uppercase alphabetic characters.
    - **Lowercase alphabetic characters** - If enabled, the password must contain lowercase alphabetic characters.
    - **Numeric characters** - If enabled, the password must contain numeric characters.
    - **Non alphanumeric characters** - If enabled, the password must contain non alphanumeric characters.
- **Password must be different from the previous (n) versions** - If enabled, the password must be different from the previous n versions (default = 1, range = 1 to 99).

[Back to Top]

Password Lifetime Options

- **Following a change of password** - Use these options to set restrictions on the lifetime of administrator passwords. The value n represents the number of days that passed since the last time the password was changed.
    - **The password will require change after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS requires a change of password due to password age (default = 30). The range is 1 to 365.
    - **The Administrator will be locked out after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS locks out the associated administrator account due to password age (default = 60, range = 1 to 365).

[Back to Top]

Password Inactivity Options

- **Following last account activity** - Use these options to place restrictions on the use of inactive administrator accounts. The value n represents the number of days that passed since the activity (administrator login).
    - **The password will require change after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS requires a change of password due to password age (default = 30). The range is 1 to 365.
    - **The Administrator will be locked out after (X) days** - Following a change of password, if enabled, x specifies the number of days before ACS locks out the associated administrator account due to password age (default = 60, range = 1 to 365).

[Back to Top]

Incorrect Password Attempt Options

Lock out Administrator after (x) successive failed attempts - Enable this option to lock out an administrator after a (x) successive failed login attempts. The ***x*** box cannot be set to zero. The default value is 3. If the Account Never Expires option is enabled for a specific administrator, this option is ignored.

[Back to Top]

291591

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Passwords are not readable within Cisco Secure ACS; it uses strong cryptography.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Through company policy inactive users should be removed or disabled every 90 days. As shown in Figure 5-51, Cisco Secure ACS password policy also enables setting of an inactivity option where an administrator will be locked out after 90 days of inactivity.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  The password lifetime option must be enabled configured to require users to change their password every 90 days. This setting can be configured as shown in Figure 5-51.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The default password policy for length specifies a minimum password length of 4 characters; this must be changed to 7 characters, as shown in Figure 5-51.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The password policy must be updated to require both alphabetic and numeric characters, as shown in Figure 5-51.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  The password history option must be enabled and configured and set to 4 versions, as shown in Figure 5-51.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  The Incorrect Password Attempt Options must be enabled and the default of 3 attempts must be changed to 6 successive failed authentications attempts, as shown in Figure 5-51.

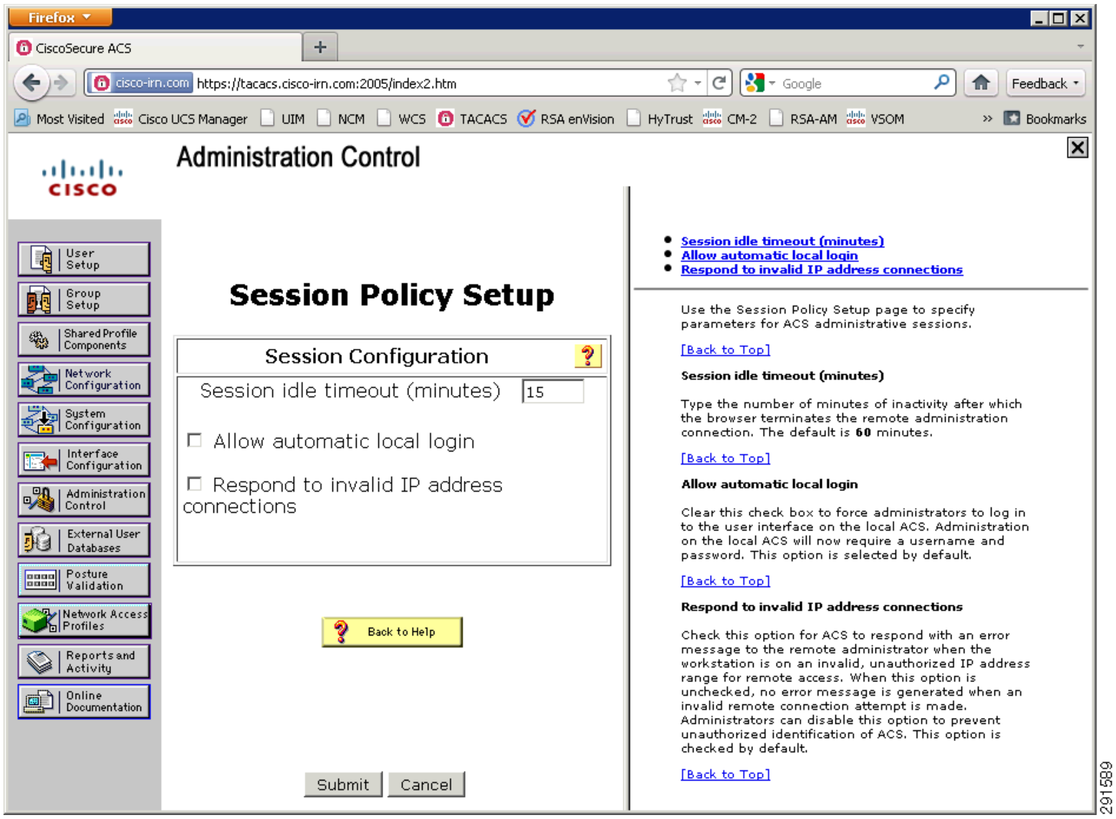
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  By default, Cisco Secure ACS requires another administrator to re-enable locked out accounts.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco Secure ACS supports session policies under the Administration Control/Session tab. Change the Session Time-out to 15 minutes from the default 60 minutes, as shown in Figure 5-52.

Figure 5-52 Session Timeout



Administration Control

Session Policy Setup

Session Configuration

Session idle timeout (minutes) 15

□ Allow automatic local login

□ Respond to invalid IP address connections

- Session idle timeout (minutes)
- Allow automatic local login
- Respond to invalid IP address connections

Use the Session Policy Setup page to specify parameters for ACS administrative sessions.

[Back to Top]

Session idle timeout (minutes)

Type the number of minutes of inactivity after which the browser terminates the remote administration connection. The default is **60** minutes.

[Back to Top]

Allow automatic local login

Clear this check box to force administrators to log in to the user interface on the local ACS. Administration on the local ACS will now require a username and password. This option is selected by default.

[Back to Top]

Respond to invalid IP address connections

Check this option for ACS to respond with an error message to the remote administrator when the workstation is on an invalid, unauthorized IP address range for remote access. When this option is unchecked, no error message is generated when an invalid remote connection attempt is made. Administrators can disable this option to prevent unauthorized identification of ACS. This option is checked by default.

[Back to Top]

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Secure ACS is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*

- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Secure ACS uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4**—*Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

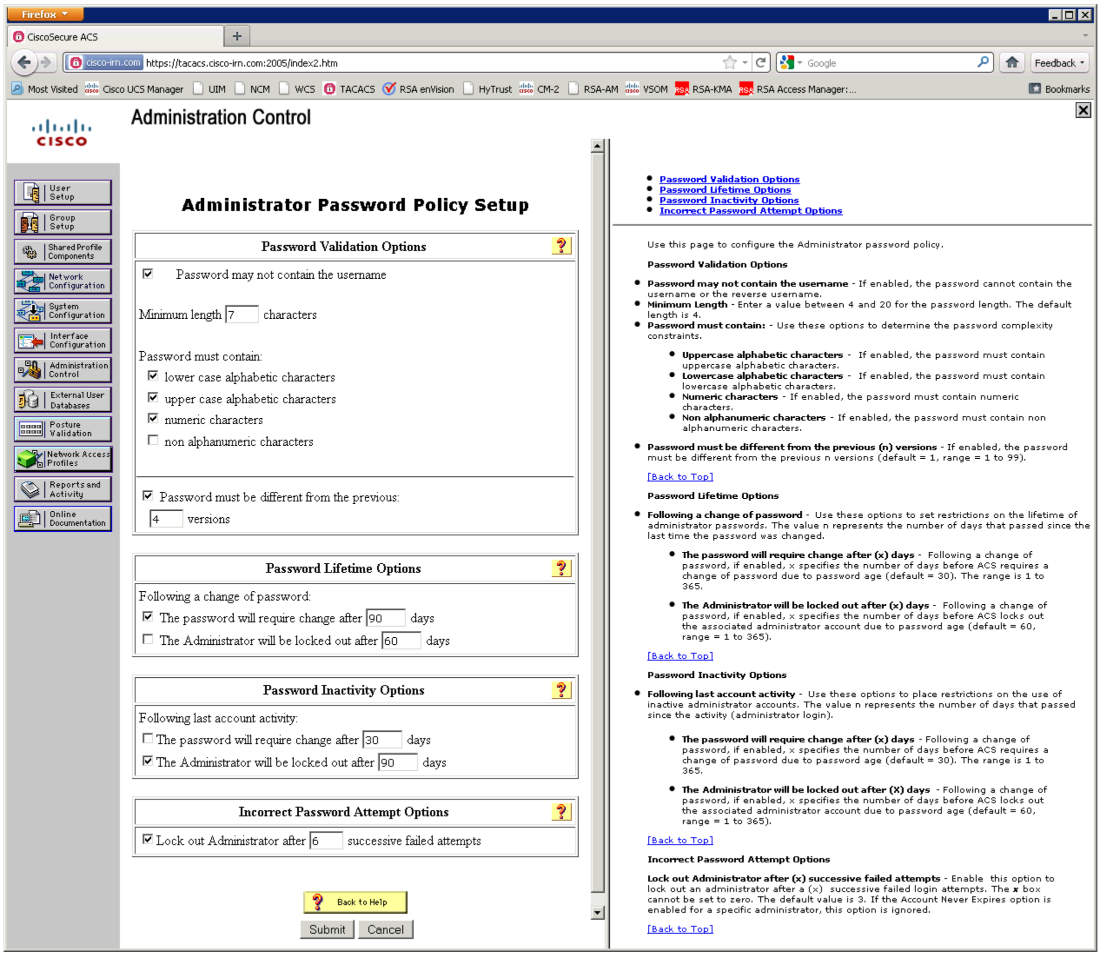
Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

Cisco Secure ACS can be configured to send its log data to the RSA enVision log management platform to meet the above requirements. The configuration procedure is documented in the RSA enVision Event Source Configuration Guide for Cisco Secure ACS, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/).

RSA enVision requires that specific attributes for each reporting function to be specified and configured in a particular order. Figure 5-53 shows the required items for generating Syslog Passed Authentications. Settings for other event types are available in the RSA enVision Event Source Configuration Guide for Cisco Secure ACS.

Figure 5-53 Syslog for Passed Authentications



Administration Control

Administrator Password Policy Setup

Password Validation Options

☑ Password may not contain the username

Minimum length 7 characters

Password must contain:

☑ lower case alphabetic characters
☑ upper case alphabetic characters
☑ numeric characters
☐ non alphanumeric characters

☑ Password must be different from the previous:
4 versions

Password Lifetime Options

Following a change of password:
☑ The password will require change after 90 days
☐ The Administrator will be locked out after 60 days

Password Inactivity Options

Following last account activity:
☐ The password will require change after 30 days
☑ The Administrator will be locked out after 90 days

Incorrect Password Attempt Options

☑ Lock out Administrator after 6 successive failed attempts

- Password Validation Options
- Password Lifetime Options
- Password Inactivity Options
- Incorrect Password Attempt Options

Use this page to configure the Administrator password policy.

Password Validation Options

- **Password may not contain the username** - If enabled, the password cannot contain the username or the reverse username.
- **Minimum Length** - Enter a value between 4 and 20 for the password length. The default length is 4.
- **Password must contain:** - Use these options to determine the password complexity constraints.
  - **Uppercase alphabetic characters** - If enabled, the password must contain uppercase alphabetic characters.
  - **Lowercase alphabetic characters** - If enabled, the password must contain lowercase alphabetic characters.
  - **Numeric characters** - If enabled, the password must contain numeric characters.
  - **Non alphanumeric characters** - If enabled, the password must contain non alphanumeric characters.
- **Password must be different from the previous (n) versions** - If enabled, the password must be different from the previous n versions (default = 1, range = 1 to 99).

[Back to Top]

Password Lifetime Options

- **Following a change of password** - Use these options to set restrictions on the lifetime of administrator passwords. The value n represents the number of days that passed since the last time the password was changed.
  - **The password will require change after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS requires a change of password due to password age (default = 30). The range is 1 to 365.
  - **The Administrator will be locked out after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS locks out the associated administrator account due to password age (default = 60, range = 1 to 365).

[Back to Top]

Password Inactivity Options

- **Following last account activity** - Use these options to place restrictions on the use of inactive administrator accounts. The value n represents the number of days that passed since the activity (administrator login).
  - **The password will require change after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS requires a change of password due to password age (default = 30). The range is 1 to 365.
  - **The Administrator will be locked out after (X) days** - Following a change of password, if enabled, x specifies the number of days before ACS locks out the associated administrator account due to password age (default = 60, range = 1 to 365).

[Back to Top]

Incorrect Password Attempt Options

Lock out Administrator after (x) successive failed attempts - Enable this option to lock out an administrator after a (x) successive failed login attempts. The ***x*** box cannot be set to zero. The default value is 3. If the Account Never Expires option is enabled for a specific administrator, this option is ignored.

[Back to Top]

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

RSA Authentication Manager

RSA Authentication Manager is the management component of the RSA SecurID®, a two-factor authentication solution, which provides a much more reliable level of user authentication than reusable passwords. SecurID authentication is based on something you know (a password or PIN) and something you have (an authenticator), and can be used to achieve compliance to PCI requirement 8.3, which requires two-factor authentication for remote access to the network by employees, administrators, and third parties. As the management component, RSA Authentication Manager is used to verify authentication requests and centrally administer authentication policies for enterprise networks.

Table 5-20 PCI Assessment Summary—RSA Authentication Manager

Models Assessed	
RSA Authentication Manager 7.1 Service Pack 2	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.3, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of RSA Authentication Manager is to securely authenticate remote users using two-factor authentication.

Table 5-20 lists the component assessment details for RSA Authentication Manager.

Table 5-21 Component Capability Assessment—RSA Authentication Manager

RSA Authentication Manager	
PRIMARY FUNCTION	**Requirement 8 (8.3)**
Securely authenticate remote users using two-factor authentication.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

RSA Authentication Manager stores and processes highly sensitive authentication information and should be deployed and operated in a secure manner. Detailed recommendations are found in the RSA Authentication Manager Security Best Practices Guide, which can be downloaded from RSA Secure Care Online (https://knowledge.rsasecurity.com/).

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are no unnecessary services enabled by default on RSA Authentication Manager. RSA Authentication Manager should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  RSA Authentication Manager should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  RSA Authentication Manager web consoles are protected with SSL.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  RSA Authentication Manager publishes security patches on RSA Secure Care Online (https://knowledge.rsasecurity.com/) in accordance with industry best practices to manage and respond to security vulnerabilities to minimize customers' risk of exposure.

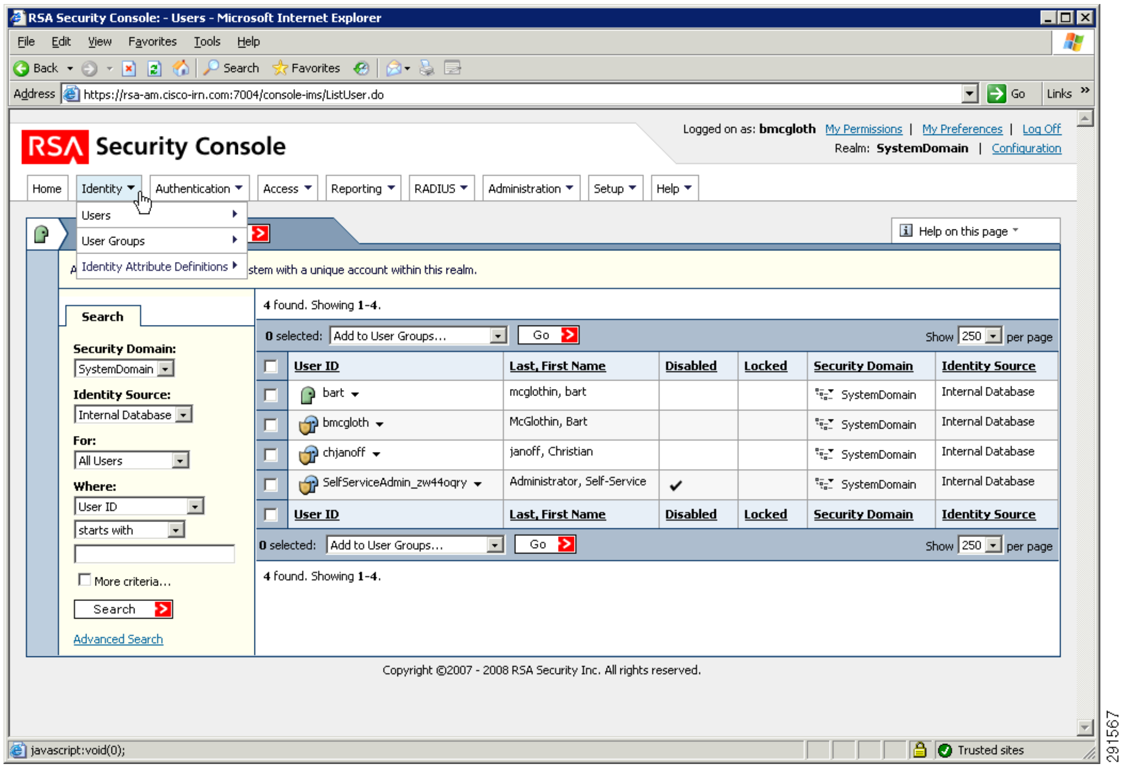
Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the RSA Authentication Manager's internal database. RSA Authentication Manager also supports linking to a centralized user database such as Active Directory using LDAP. Within RSA Authentication Manager, individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

RSA Authentication Manager has powerful access control capabilities to limit access to system components and cardholder data based on user role or group membership. Users and groups are created under the Identity tab of the Security console, as shown in Figure 5-54.

Figure 5-54 Users and Groups


RSA Security Console: - Users - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://rsa-am.cisco-irn.com:7004/console-ims/ListUser.do
Go Links
RSA Security Console
Home Identity Authentication Access Reporting RADIUS Administration Setup Help
Users
User Groups
Identity Attribute Definitions
Help on this page
291567

Logged on as: **bmcgloth** My Permissions | My Preferences | Log Off
Realm: **SystemDomain** | Configuration

A ...stem with a unique account within this realm.

Search

Security Domain: SystemDomain

Identity Source: Internal Database

For: All Users

Where: User ID, starts with

□ More criteria...

Search

Advanced Search

4 found. Showing **1-4**.

0 selected: Add to User Groups... Go Show 250 per page

□	User ID	Last, First Name	Disabled	Locked	Security Domain	Identity Source
□	bart	mcglothin, bart			SystemDomain	Internal Database
□	bmcgloth	McGlothin, Bart			SystemDomain	Internal Database
□	chjanoff	janoff, Christian			SystemDomain	Internal Database
□	SelfServiceAdmin_zw44oqry	Administrator, Self-Service	✓		SystemDomain	Internal Database

0 selected: Add to User Groups... Go Show 250 per page

4 found. Showing **1-4**.

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

javascript:void(0); Trusted sites

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

RSA Authentication Manager's access control system defaults to deny access.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database as shown below.

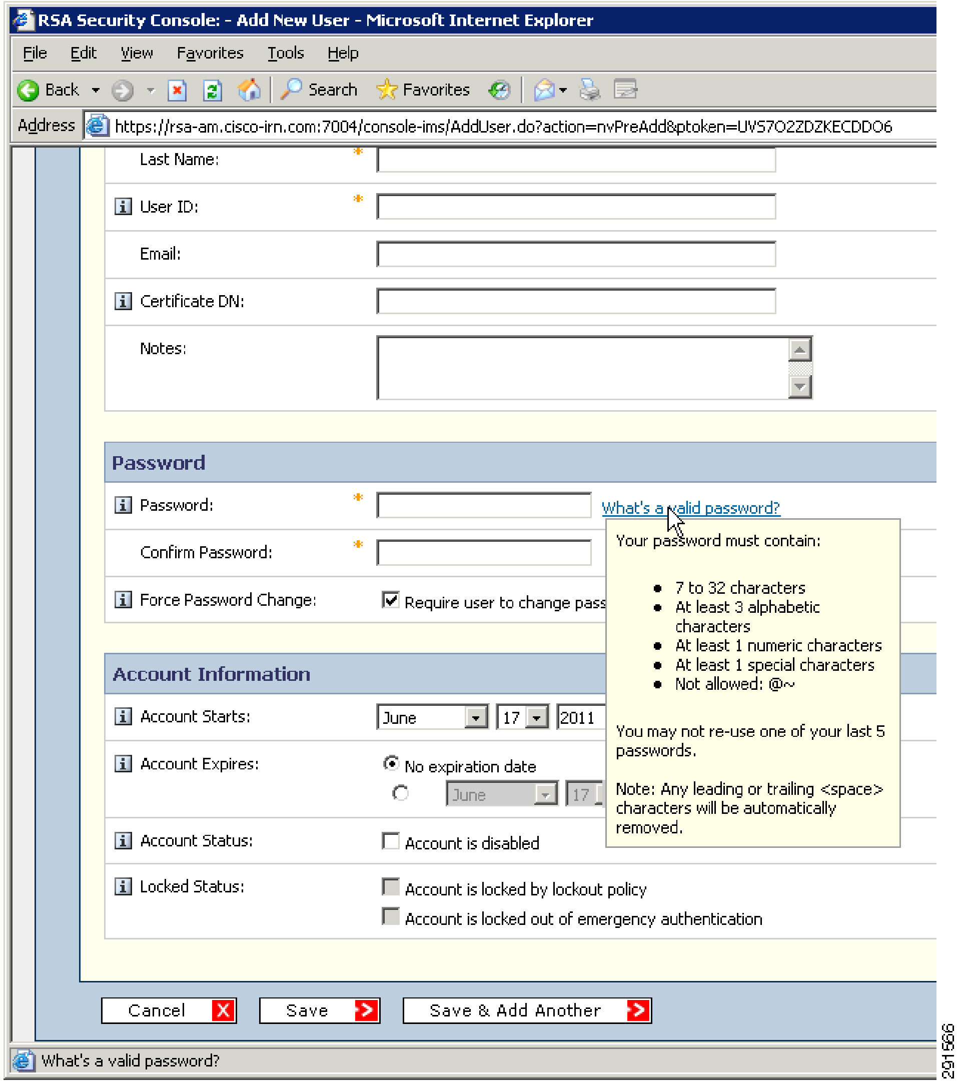
- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  RSA Authentication Manager supports the creation of local users or linking to a central repository of users. Through company policy, each user must be assigned a unique ID.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts in RSA Authentication Manager require setting of a password according to the assigned password policy as shown in Figure 5-55.

Figure 5-55 User Password Requirements Based on Policy


RSA Security Console: - Add New User - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://rsa-am.cisco-irn.com:7004/console-ims/AddUser.do?action=nvPreAdd&ptoken=UVS7O2ZDZKECDDO6
Cancel
Save
Save & Add Another
What's a valid password?
291566

Last Name: *	
User ID: *	
Email:	
Certificate DN:	
Notes:	

Password

Password: *	What's a valid password?
Confirm Password: *	
Force Password Change:	☑ Require user to change pass

Your password must contain:

- 7 to 32 characters
- At least 3 alphabetic characters
- At least 1 numeric characters
- At least 1 special characters
- Not allowed: @~

You may not re-use one of your last 5 passwords.

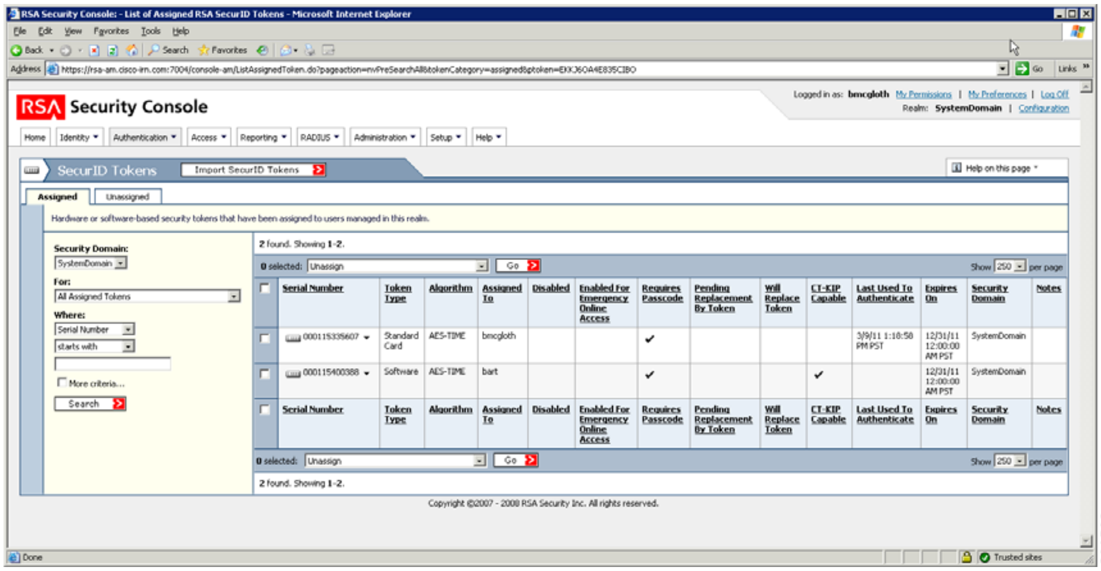
Note: Any leading or trailing <space> characters will be automatically removed.

Account Information

Account Starts:	June 17 2011
Account Expires:	● No expiration date ○ June 17
Account Status:	□ Account is disabled
Locked Status:	□ Account is locked by lockout policy □ Account is locked out of emergency authentication

Additional authentication tokens can also be assigned to each user, as shown in Figure 5-56.

Figure 5-56 Assigned Tokens


RSA Security Console: - List of Assigned RSA SecurID Tokens - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://rsa-am.cisco-irn.com:7004/console-am/ListAssignedToken.do?pageaction=nvPreSearchAll&tokenCategory=assigned&ptoken=EKKJ6OA4E835CIBO
Go Links
RSA Security Console
Logged in as: bmcgloth My Permissions | My Preferences | Log Off
Realm: SystemDomain | Configuration
Home Identity Authentication Access Reporting RADIUS Administration Setup Help
SecurID Tokens
Import SecurID Tokens
Help on this page
Assigned Unassigned
Search
Go
Done
Trusted sites
291563

Hardware or software-based security tokens that have been assigned to users managed in this realm.

Security Domain: SystemDomain

For: All Assigned Tokens

Where: Serial Number starts with

□ More criteria...

2 found. Showing 1-2.

0 selected: Unassign Show 250 per page

□	Serial Number	Token Type	Algorithm	Assigned To	Disabled	Enabled For Emergency Online Access	Requires Passcode	Pending Replacement By Token	Will Replace Token	CT-KIP Capable	Last Used To Authenticate	Expires On	Security Domain	Notes
□	000115335607	Standard Card	AES-TIME	bmcgloth			✓				3/9/11 1:18:58 PM PST	12/31/11 12:00:00 AM PST	SystemDomain	
□	000115400388	Software	AES-TIME	bart			✓			✓		12/31/11 12:00:00 AM PST	SystemDomain	
□	Serial Number	Token Type	Algorithm	Assigned To	Disabled	Enabled For Emergency Online Access	Requires Passcode	Pending Replacement By Token	Will Replace Token	CT-KIP Capable	Last Used To Authenticate	Expires On	Security Domain	Notes

0 selected: Unassign Show 250 per page

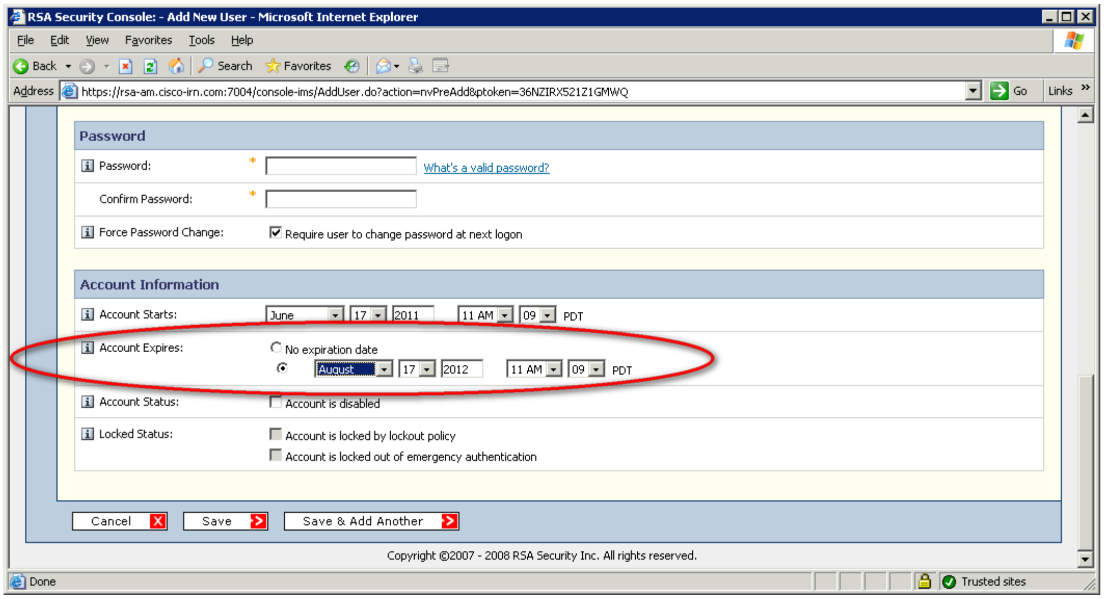
2 found. Showing 1-2.

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

- **PCI 8.3**—*Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) Note: Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Through company policy, inactive users should be removed or disabled every 90 days. RSA Authentication Manager also enables setting of an account expiration date for individual accounts, as shown in Figure 5-57.

Figure 5-57 User Account Expiration


RSA Security Console: - Add New User - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://rsa-am.cisco-irn.com:7004/console-ims/AddUser.do?action=nvPreAdd&ptoken=36NZIRX521Z1GMWQ
Go Links
Done
Trusted sites
291565

Password

Password: * What's a valid password?

Confirm Password: *

Force Password Change: ☑ Require user to change password at next logon

Account Information

Account Starts: June 17 2011 11 AM 09 PDT

Account Expires: ○ No expiration date
● August 17 2012 11 AM 09 PDT

Account Status: □ Account is disabled

Locked Status: □ Account is locked by lockout policy
□ Account is locked out of emergency authentication

Cancel Save Save & Add Another

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

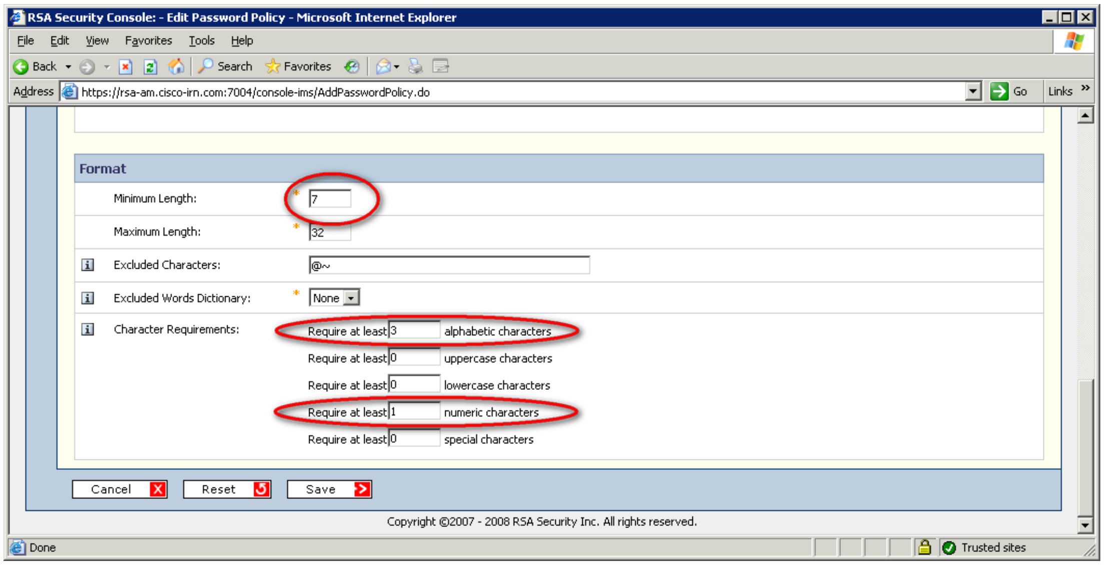
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  The default Initial Password Policy is created when a new realm is established, and requires users to change their passwords every 90 days.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The default Initial Password Policy must be updated to set a minimum password length of 7 characters, as shown in Figure 5-58.

Figure 5-58 Initial Password Policy


RSA Security Console: - Edit Password Policy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://rsa-am.cisco-irn.com:7004/console-ims/AddPasswordPolicy.do
Go Links
Done
Trusted sites
291560

Format

Minimum Length: * 7

Maximum Length: * 32

Excluded Characters: @~

Excluded Words Dictionary: * None

Character Requirements: Require at least 3 alphabetic characters
Require at least 0 uppercase characters
Require at least 0 lowercase characters
Require at least 1 numeric characters
Require at least 0 special characters

Cancel Reset Save

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The default Initial Password Policy must be updated to require both alphabetic and numeric characters, as shown in Figure 5-58.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  The default Initial Password Policy is created when a new realm is established, and restricts users from re-using their last five passwords.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

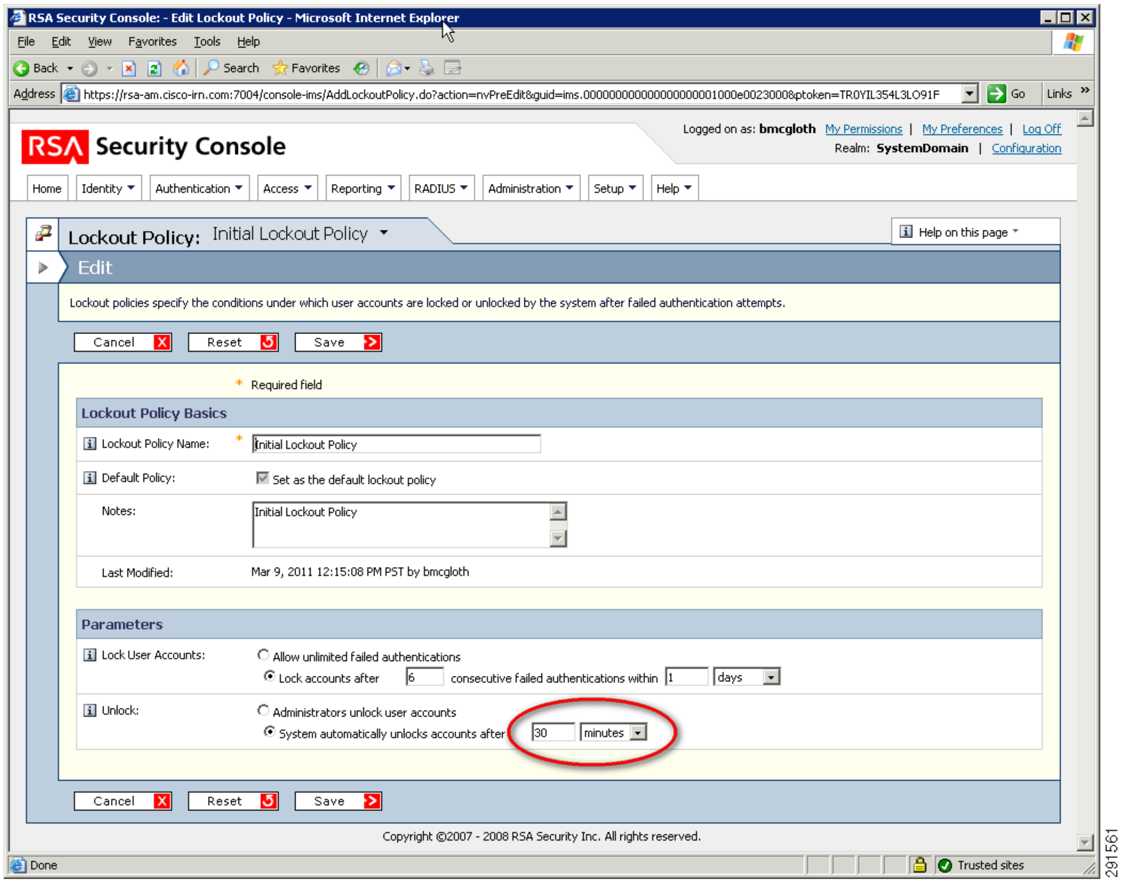
  The Initial Lockout policy is enabled by default and locks accounts after six consecutive failed authentications within one day.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  The Initial Lockout policy is enabled by default; the only change for PCI compliance is to change the auto-unlock parameter from 15 minutes to 30 minutes. This change is made under the Authentication > Policies > Lockout Policies.

  Figure 5-59 shows an appropriate policy for PCI compliance.

Figure 5-59 Revised Initial Lockout Policy Edited for PCI


RSA Security Console: - Edit Lockout Policy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://rsa-am.cisco-irn.com:7004/console-ims/AddLockoutPolicy.do?action=nvPreEdit&guid=ims.000000000000000000001000e0023000&ptoken=TR0YIL354L3LO91F
Go Links
RSA Security Console
Logged on as: bmcgloth My Permissions | My Preferences | Log Off
Realm: SystemDomain | Configuration
Home Identity Authentication Access Reporting RADIUS Administration Setup Help
Help on this page
Edit
Cancel Reset Save
Done Trusted sites
291561

Lockout Policy: Initial Lockout Policy

Lockout policies specify the conditions under which user accounts are locked or unlocked by the system after failed authentication attempts.

* Required field

Lockout Policy Basics

Lockout Policy Name: * Initial Lockout Policy

Default Policy: ☑ Set as the default lockout policy

Notes: Initial Lockout Policy

Last Modified: Mar 9, 2011 12:15:08 PM PST by bmcgloth

Parameters

Lock User Accounts: ○ Allow unlimited failed authentications
● Lock accounts after 6 consecutive failed authentications within 1 days

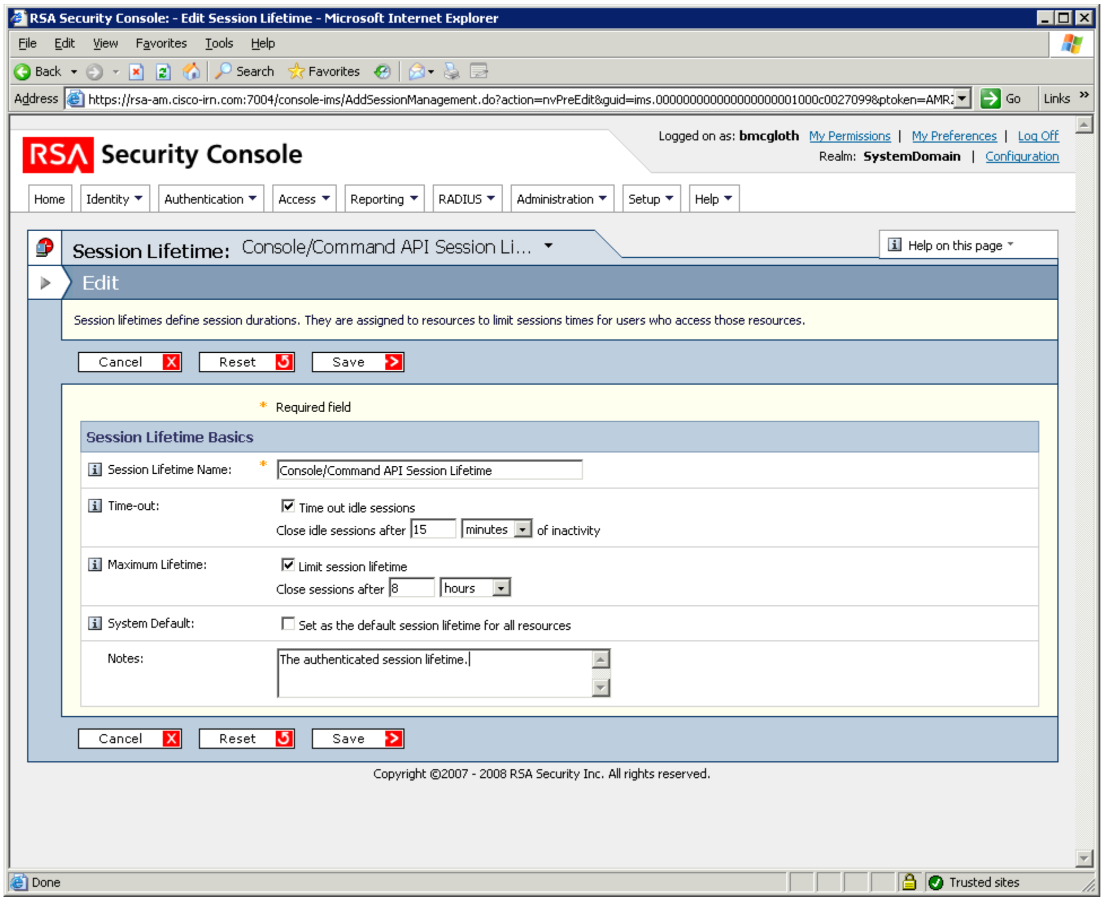
Unlock: ○ Administrators unlock user accounts
● System automatically unlocks accounts after 30 minutes

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  RSA Authentication Manager supports session policies under the Access tab. Change the Session Time-out for the Console/Command API to 15 minutes from the default, as shown in Figure 5-60.

Figure 5-60 Session Lifetime for Console


RSA Security Console: - Edit Session Lifetime - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://rsa-am.cisco-irn.com:7004/console-ims/AddSessionManagement.do?action=nvPreEdit&guid=ims.000000000000000000001000c0027099&ptoken=AMR:
Go Links
RSA Security Console
Logged on as: bmcgloth My Permissions | My Preferences | Log Off
Realm: SystemDomain | Configuration
Home Identity Authentication Access Reporting RADIUS Administration Setup Help
Help on this page
Cancel Reset Save
Done Trusted sites
291564

Session Lifetime: Console/Command API Session Li...

Edit

Session lifetimes define session durations. They are assigned to resources to limit sessions times for users who access those resources.

* Required field

Session Lifetime Basics

Session Lifetime Name: * Console/Command API Session Lifetime

Time-out: ☑ Time out idle sessions
Close idle sessions after 15 minutes of inactivity

Maximum Lifetime: ☑ Limit session lifetime
Close sessions after 8 hours

System Default: ☐ Set as the default session lifetime for all resources

Notes: The authenticated session lifetime.

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

RSA Authentication Manager has very powerful and flexible capabilities to define password and account lockout policies to meet all of the above criteria.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

RSA Authentication Manager is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*

- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

RSA Authentication Manager uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

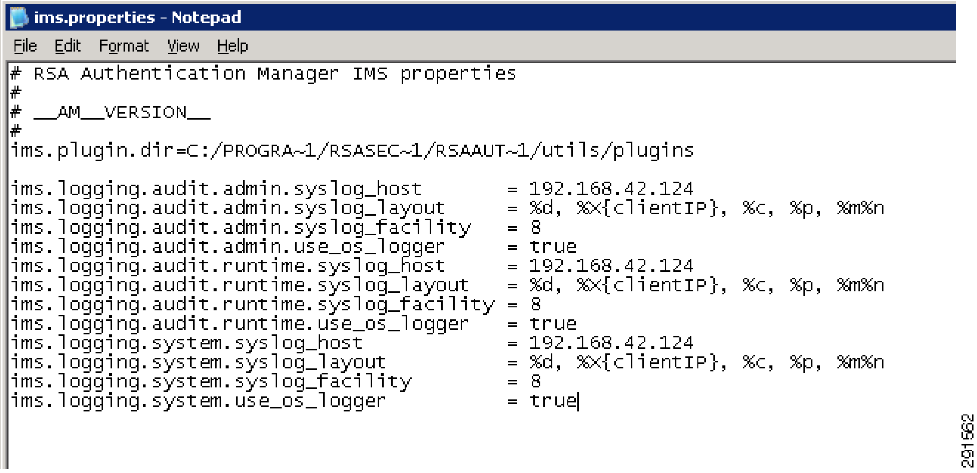
- **PCI 10.5**—*Secure audit trails so they cannot be altered.*

  Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  RSA Authentication Manager can be configured to send its log data to the RSA enVision log management platform to meet the above requirements. The configuration procedure is documented in the enVision Event Source Configuration Guide for RSA Authentication Manager, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/). One step is editing the IMS.Properties file, as shown in Figure 5-61.

Figure 5-61 IMS Properties File



```
# RSA Authentication Manager IMS properties
#
# __AM__VERSION__
#
ims.plugin.dir=C:/PROGRA~1/RSASEC~1/RSAAUT~1/utils/plugins

ims.logging.audit.admin.syslog_host       = 192.168.42.124
ims.logging.audit.admin.syslog_layout     = %d, %X{clientIP}, %c, %p, %m%n
ims.logging.audit.admin.syslog_facility   = 8
ims.logging.audit.admin.use_os_logger     = true
ims.logging.audit.runtime.syslog_host     = 192.168.42.124
ims.logging.audit.runtime.syslog_layout   = %d, %X{clientIP}, %c, %p, %m%n
ims.logging.audit.runtime.syslog_facility = 8
ims.logging.audit.runtime.use_os_logger   = true
ims.logging.system.syslog_host            = 192.168.42.124
ims.logging.system.syslog_layout          = %d, %X{clientIP}, %c, %p, %m%n
ims.logging.system.syslog_facility        = 8
ims.logging.system.use_os_logger          = true
```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco TrustSec

Cisco TrustSec, the security component of the Cisco Borderless Network architecture, provides visibility and control into who and what is connected to the network. Cisco TrustSec allows organizations to embrace the rapidly changing business environment of mobility, virtualization, and collaboration while enforcing compliance, maintaining data integrity and confidentiality, and establishing a consistent global access policy. Cisco TrustSec allows businesses to gain complete control over the access points into their networks. This includes all wired, wireless, and VPN network entry points.

Cisco TrustSec ensures that you know what devices and users are on your network, and that those devices and users comply with your security policies via the following components:

- Cisco Identity Services Engine (ISE)—The Cisco ISE is a next-generation policy manager that delivers authentication, authorization, and accounting (AAA); posture; profiling; and guest management services on a single platform. The Cisco ISE automatically discovers and classifies endpoints, provides the right level of access based on identity, and provides the ability to enforce endpoint compliance by checking a device's posture. The Cisco ISE also provides advanced authorization and enforcement capabilities, including Security Group Access (SGA) through the use of security group tags (SGTs) and security group access control lists (ACLs). Administrators can centrally create and manage access control policies for users and endpoints in a consistent fashion, and gain end-to-end visibility into everything that is connected to the network.
- Cisco TrustSec Identity on Cisco Networking Infrastructure—Identity-based networking services on the Cisco routing, switching and wireless infrastructure provides the ability to authenticate users and devices via features such as 802.1x, MAC authentication bypass (MAB), and Web Authentication. In addition, this same infrastructure enforces the appropriate access into parts of the network via VLANs, downloadable or named ACLs, and security group ACLs.

- Client—Cisco AnyConnect VPN Client is a software client that enables you to deploy a single 802.1x authentication framework to access wired and wireless networks while the Cisco NAC agent delivers endpoint posture information. The Cisco TrustSec architecture also supports native OS supplicants.

The Cisco TrustSec solution offers the following benefits:

- Allows enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise
- Prevents unauthorized network access to protect corporate assets
- Provides complete guest lifecycle management by empowering sponsors to on-board guests, thus reducing IT workload
- Discovers, classifies, and controls endpoints connecting to the network to enable the appropriate services per endpoint type
- Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention
- Offers a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations.

Figure 5-62 shows an example of a Cisco ISE-based TrustSec LAN deployment.

Figure 5-62 Cisco ISE-Based TrustSec LAN Deployment

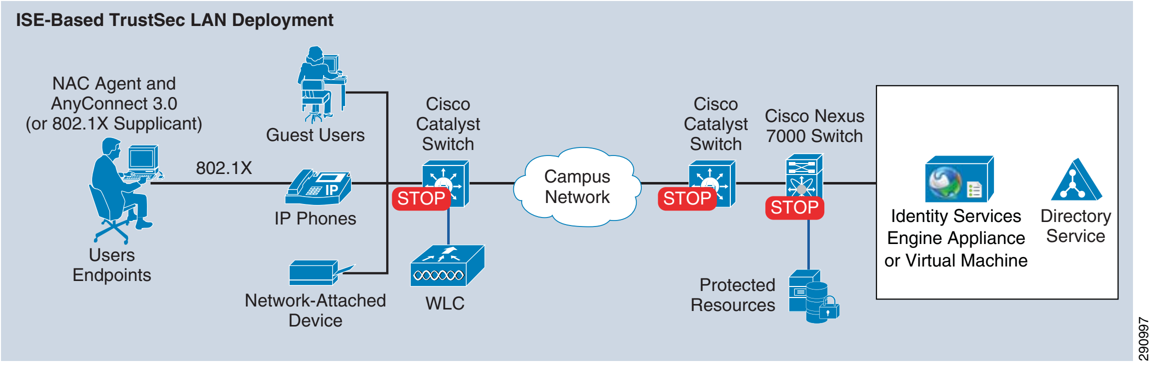


Table 5-22 PCI Assessment Summary—Cisco Identity Services Engine

Models Assessed	
Cisco Identity Service Engine version 1.0.3.377	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 9	9.1.2
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI 11	11.1.b, 11.1.d

Table 5-22 PCI Assessment Summary—Cisco Identity Services Engine (continued)

PCI Sub-Requirements Requiring Compensating Controls
No compensating controls were required to satisfy any sub-requirements.
PCI Sub-Requirements Failed
No sub-requirements were failed.

Primary PCI Function

Cisco ISE and TrustSec identity features detect and prevent rogue wireless devices from connecting to in-scope PCI networks (11.1); in addition, Cisco ISE locks down publicly accessible network ports to only authorized devices and users (9.1.2). In addition to its primary focus, Cisco ISE can also help with compliance and enforcement of requirements 6.1, 7.1, 7.2, 8.3, 8.5, and 10.

Table 5-22 lists the component assessment details for the Cisco TrustSec Solution.

Table 5-23 Component Capability Assessment—Cisco TrustSec

Cisco TrustSec	
PRIMARY FUNCTION	**Requirement 7, 11 (7.1, 7.2, 11.1)**
Authenticate and authorize users and endpoints via wired, wireless, and VPN.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

For the purposes of this guide, Cisco ISE is configured to authenticate individual users and ISE Admin users using Active Directory (AD). Cisco ISE is also used to profile and assess the posture of individual wired and wireless devices to ensure that they comply with the PCI standard. Cisco ISE relies on

TrustSec wired and wireless identity features such as 802.1x, MAB, and web portal authentication on Cisco infrastructure to collect user identity information. It relies on the Cisco ISE NAC agent and the Cisco ISE profiler engine to collect posture and profiling information from devices. Note the following:

- The solution tested used the virtual machine appliance version of Cisco ISE running on an ESX platform.
- The default accounts for administration are removed.
- HTTPS is enabled and HTTP disabled.
- Cisco ISE communicates with the Cisco switches and wireless controllers using RADIUS.
- Cisco ISE can use dynamic VLAN and port or VLAN access control rules to provide PCI segmentation of a network. For example, members of the PCI active directory group are automatically moved to the PCI VLAN when they connect to the network. Cisco ISE can then apply strong access lists to this VLAN or directly to the user switch port to accomplish segmentation.
- Access control rule sets must adhere to a "least amount of access necessary" policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment on the point-of-sale networks.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- The Cisco ISE system is configured to be compliance with all of the access controls, logging controls, and other general system controls required by PCI DSS 2.0.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure. (For example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.)*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

  The Cisco Identity Service Engine appliance does not allow changes to the operating system, to the database, installation of unsupported hardware, or of unsupported third-party software.

  The Cisco ISE management console supports only HTTPS access.

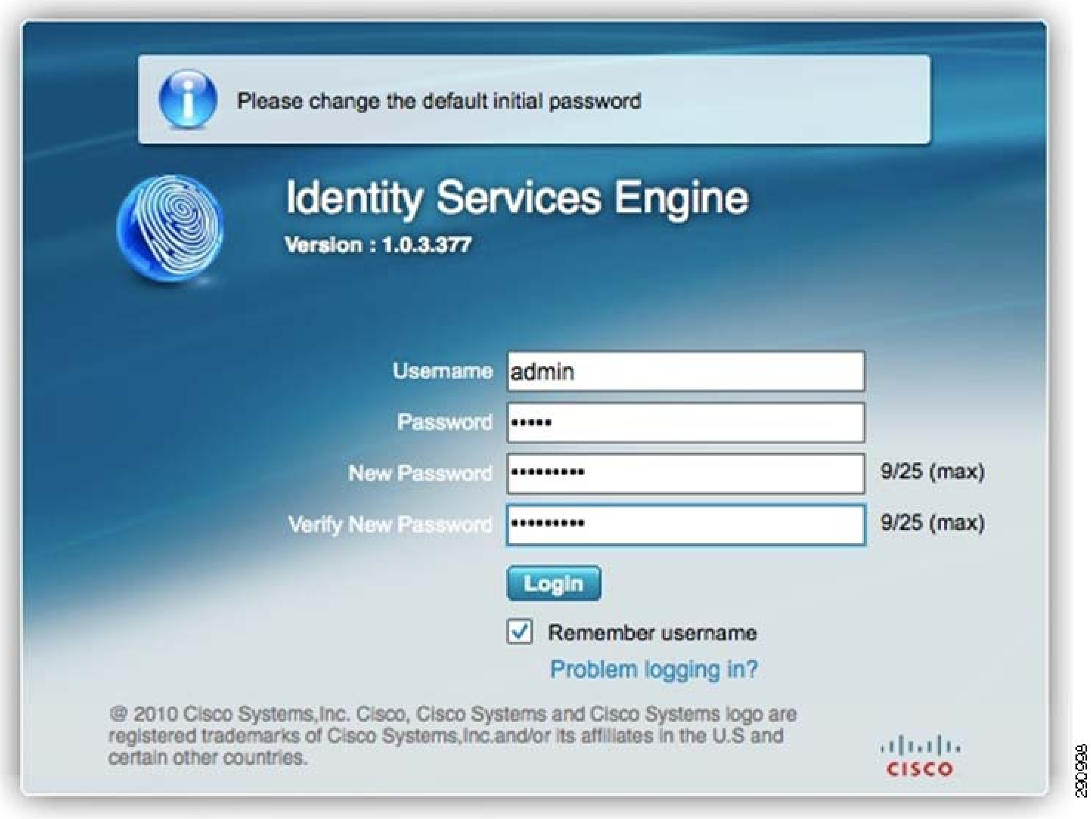
  Cisco ISE is configured to use SSL as a highly secure management portal technology.

  Role-based administration is configured for administrative tasks.

  Cisco ISE was locked down according to generally accepted industry standards and the above PCI requirements.

  Figure 5-63 shows the Cisco ISE login screen.

Figure 5-63 Cisco ISE Login



Please change the default initial password

Identity Services Engine

Version : 1.0.3.377

Username: admin

Password: •••••

New Password: ••••••••• 9/25 (max)

Verify New Password: ••••••••• 9/25 (max)

Login
☑ Remember username
Problem logging in?
@ 2010 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc.and/or its affiliates in the U.S and certain other countries.
CISCO
290998

Requirement 6: Develop and maintain secure systems and applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.*

Note An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices, systems, and databases) and higher than less-critical internal devices, ensuring that high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.

Cisco ISE itself has several auto-update configuration options you can use to keep it current. Cisco ISE can also be upgraded manually.

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in the Cisco Identity Service Engine. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html

More importantly, Cisco ISE is able to check all hosts connecting to the network to make sure they are compliant with requirement 6.1. Operating system patches and application patches can be enforced before allowing network access. Cisco ISE can offer remediation options to users who are out of compliance.

Requirement 7: Restrict access to cardholder data by business need to know

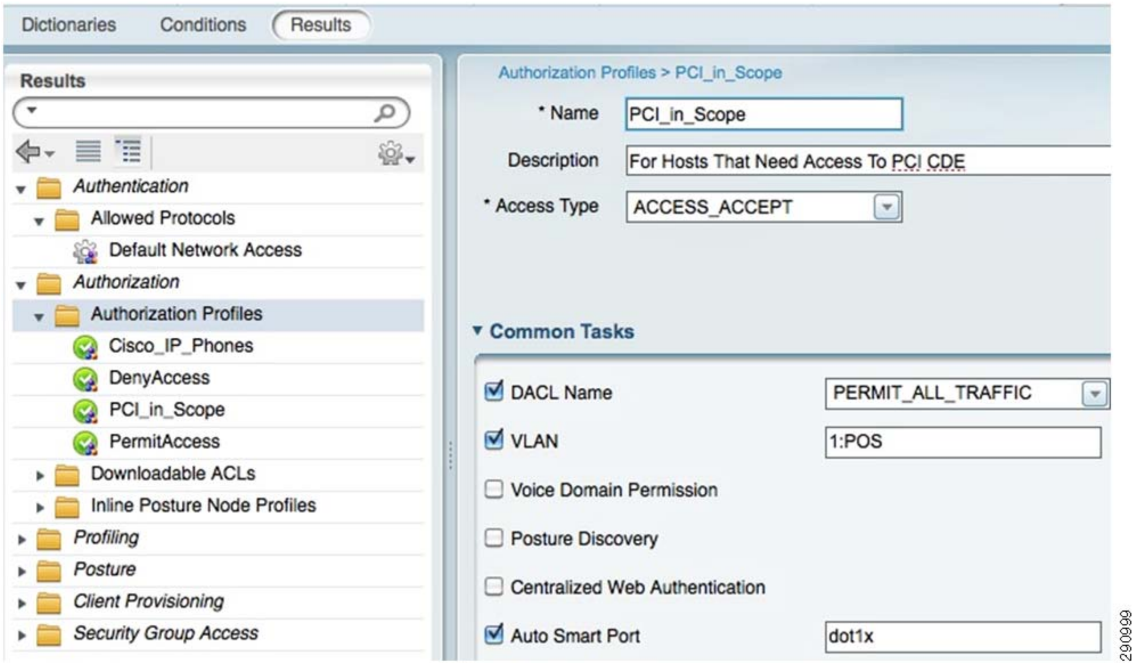
To meet all of the requirements listed below, the Cisco PCI Solution for Retail uses a centralized user database in the Active Directory. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. Cisco ISE connects to this resource via native Windows services to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function.*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system.*

TrustSec identity features and ISE ensure that only privileged users can access the CDE. This is done using the authentication credentials supplied by the wired and wireless infrastructure, along with the AD attributes of a user connecting to the network. Based on a Cisco ISE authorization profile match, that user is put onto the proper VLAN and given a group-specific port access control list to control where they can go on the network. Additionally, a Cisco SmartPort macro can be run on the switchport to ensure they have the proper configuration.

Figure 5-64 shows the Authorization Profiles screen.

Figure 5-64 Authorization Profiles



* Name: PCI_in_Scope

Description: For Hosts That Need Access To PCI CDE

* Access Type: ACCESS_ACCEPT

☑ DACL Name: PERMIT_ALL_TRAFFIC

☑ VLAN: 1:POS

□ Voice Domain Permission

□ Posture Discovery

□ Centralized Web Authentication

☑ Auto Smart Port: dot1x

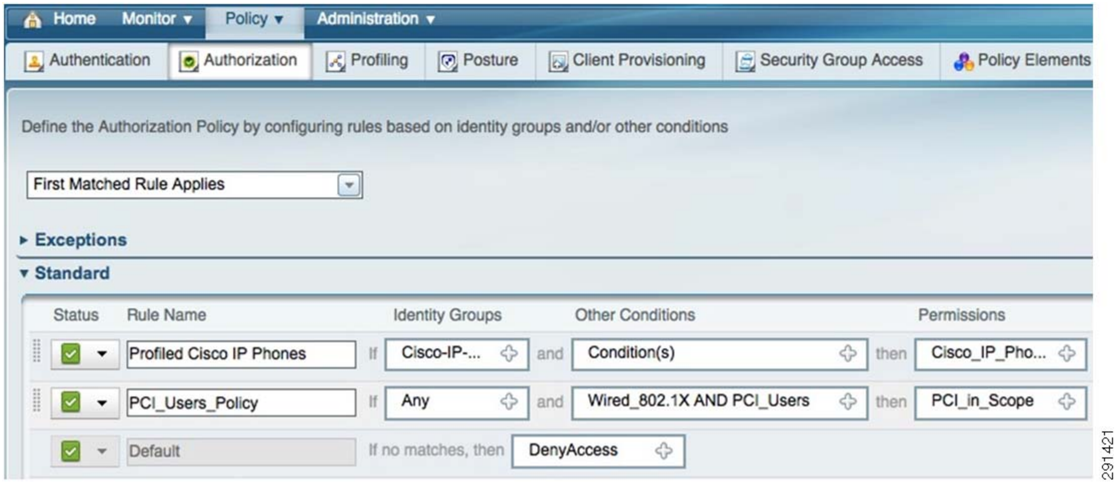
- **PCI 7.2.1**—*Coverage of all system components.*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function.*

- **PCI 7.2.3**—*Default "deny-all" setting.*

  If Cisco ISE does not explicitly match an authorization policy, network access is denied.

  Figure 5-65 shows the Authorization Policy screen.

Figure 5-65 Authorization Policy



Define the Authorization Policy by configuring rules based on identity groups and/or other conditions

First Matched Rule Applies

▸ Exceptions

▾ Standard

Status	Rule Name		Identity Groups		Other Conditions		Permissions
☑	Profiled Cisco IP Phones	If	Cisco-IP-...	and	Condition(s)	then	Cisco_IP_Pho...
☑	PCI_Users_Policy	If	Any	and	Wired_802.1X AND PCI_Users	then	PCI_in_Scope
☑	Default	If no matches, then	DenyAccess				

Requirement 8: Assign a unique ID to each person with computer access

The relevant sub-requirements below were met using the Cisco ISE linked to the windows Active Directory domain. Cisco ISE also supports linking to other authentication servers.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco ISE supports the creation of local user accounts with unique IDs through the use of the **username** command in the CLI or via the Web GUI. These can be used for local fallback user accounts if connectivity to Active directory is lost.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*

  – *Something you know, such as a password or passphrase*

  – *Something you have, such as a token device or smart card*

  – *Something you are, such as a biometric*

  When configuring local user accounts, you must specify a password to achieve PCI compliance.

  Cisco ISE can use any of the methods indicated above to authenticate RADIUS users. The audited configuration for this guide used passwords stored on an Active directory server.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*All local passwords on the Cisco ISE are stored using strong encryption

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco ISE supports tracking of a users last activity; accounts reviewed as having no activity can then be easily disabled or removed.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

The Cisco ISE password policy support the setting of a password expiration that forces the user to change their password every 90 days.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The Cisco ISE password policy is configurable to specify a minimum password length.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The Cisco ISE password policy is configurable to specify an appropriate complexity of numbers and characters.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  The Cisco ISE password policy is configurable to track and prevent the re-use of historical password as configured in the Web GUI.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Compliance with these sub-requirements regarding account lockout was achieved within the solution by implementing the LDAP/AD authentication to Microsoft Active Directory for user account services. The version of Cisco ISE that was validated does not support account lockout for 802.1x authenticated clients, or Web GUI clients.

  Authentications can occur at the switch port level on the wired infrastructure, and on wireless ports via identity features such as 802.1x, MAB, or web authentication.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco ISE is configured to re-authenticate both admin users and RADIUS users every 15 minutes.

  The following is a sample configuration of the Cisco ISE password policy from the CLI:

```
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  no-previous-password
  password-expiration-enabled
  password-expiration-days 90
  password-expiration-warning 10
  min-password-length 7
  password-lock-enabled
  password-lock-retry-count 6
```

Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.2**—*Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.*

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco ISE uses the local clock facilities of the host server on which it is installed to meet the following requirements.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco ISE uses the local clock facilities to meet the following requirements.

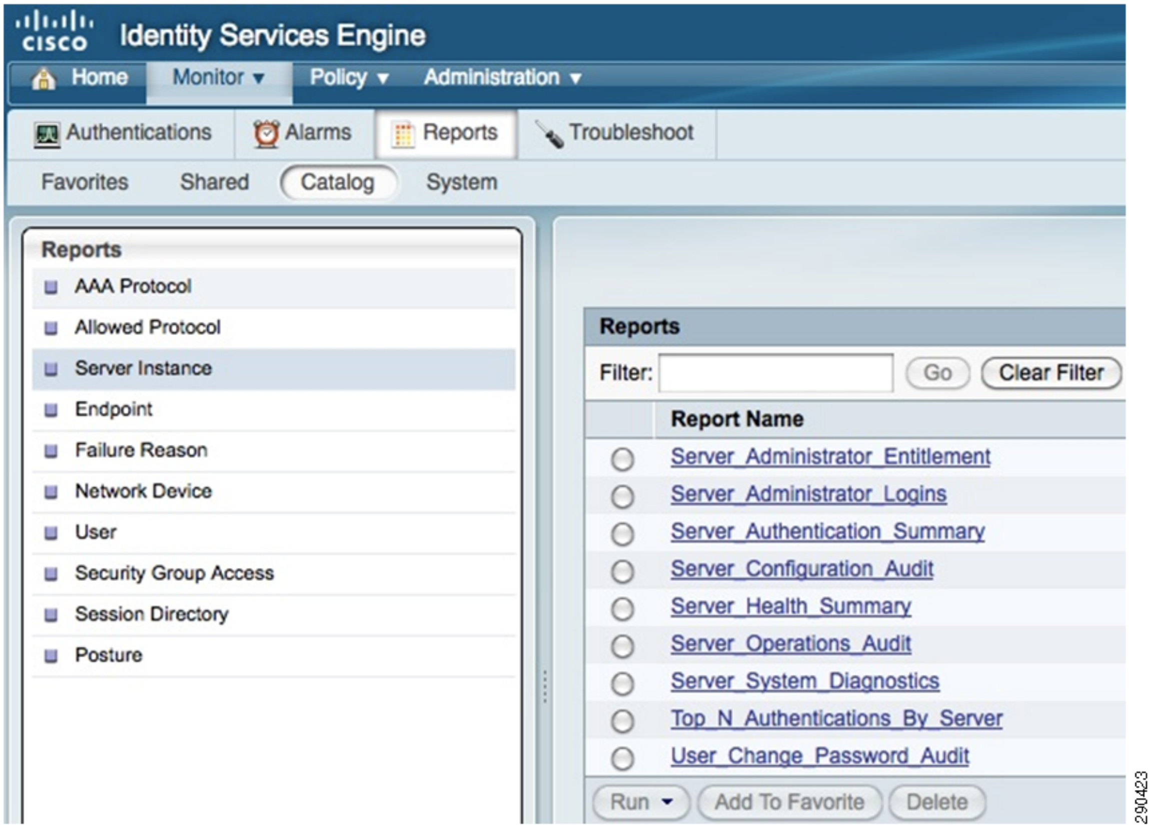
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco ISE uses NTP to meet these requirements by implementing the following configuration statement:

```
ntp server 192.168.62.161 192.168.62.162
```

Figure 5-66 shows the Server Instance screen.

Figure 5-66 Server Instance



Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  There is a robust local audit trail configured for Cisco ISE changes. Cisco ISE is configured to audit all RADIUS device access using RADIUS accounting. Note that Cisco ACS can use TACACS+ to accomplish this as well. You need not deploy both solutions.

  Audit log files are backed up daily to a backup server (RSA enVision). Cisco ISE is configured to send change logs to this server as well as provide a list of built-in and custom audit reports on the Cisco ISE system itself.

  The following is a sample configuration:

```
logging 192.168.42.124
logging loglevel 6
```

Requirement 11: Regularly test security systems and processes.

The following requirements can be addressed using Cisco network admission control.

- **PCI 11.1.b**—*Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:*
- *WLAN cards inserted into system components*
- *Portable wireless devices connected to system components (for example, by USB, etc.)*
- *Wireless devices attached to a network port or network device*
- **PCI 11.1.d**—*If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.*

  Cisco NAC capabilities can be configured on the store switches to automate the verification of approved devices being attached to the network. In addition to configuring the NAC authentication services in the data center, add the following configurations to the switch and switch interface ports where NAC is to be used (for example, publicly accessible ports):

```
Pre-requirements for NAC (domain name, name server, time settings, crypto keys):
 ip domain-name cisco-irn.com
 ip name-server 192.168.42.130
 Crypto key generate rsa 1024
 ntp server 192.168.62.161 prefer
 ntp server 192.168.62.162
 clock timezone PST -8
 clock summer-time PDT recurring
!
! ----Configurations to add for NAC ----
!
aaa new-model
!
!
aaa authentication dot1x default group radius local
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 192.168.42.111
 server-key 7 <removed>
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 5 tries 3
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
radius-server vsa send accounting
radius-server vsa send authentication
!
authentication mac-move permit
!
!
ip device tracking
ip admission name ise proxy http inactivity-time 60
!
cts sxp enable
cts sxp default source-ip 10.10.111.13 {use Switch Management IP}
!
dot1x system-auth-control
!
fallback profile ise
 ip access-group ACL-DEFAULT in
 ip admission ise
!
! ----Auto Smart Ports Macro method for port configurations-------
!
macro name dot1x
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout tx-period 5
```

Note Methods that may be used in the process include but are not limited to wireless network scans, physical site inspections, Network Admission Control (NAC), or wireless IDS/IPS.

Cisco TrustSec Identity features were enabled on the wired infrastructure to authenticate users and devices. The Cisco ISE Policy Manager was configured to not allow an unauthorized access point to connect to the wired network. Cisco ISE was also configured to detect and identify the presence of wireless USB or wireless LAN cards on PC systems acting as peer-to-peer wireless networks. Cisco ISE was configured to alert and mitigate this rogue wireless threat.

Cisco ISE was configured to profile all devices connected to the network. Any access points detected were allowed only if they were in the approved list. All wired ports were set up to authenticate and posture-assess users and devices connecting to the network switches. The device posture assessment included checks for the setup of peer-to-peer wireless network and the setup of a wireless card as an access point on the device. If either of these were true, the device would be denied network access.

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Management

Cisco Security Manager

The Cisco Security Manager is a powerful yet easy-to-use solution for configuring firewall, VPN, and IPS policies on Cisco security appliances, firewalls, routers, and switch modules.

Cisco Security Manager helps enable enterprises to manage and scale security operations efficiently and accurately. Its end-to-end tools provide consistent policy enforcement, quick troubleshooting of security events, and summarized reports from across the security deployment.

Cisco Security Manager enables you to centrally manage security policies over 250 types and models of Cisco security devices. Cisco Security Manager supports integrated provisioning of firewall, IPS, and VPN (most site-to-site, remote access, and SSL) services across the following:

- Cisco IOS/ISR/ASR routers
- Cisco Catalyst switches
- Cisco ASA and PIX security appliances
- Cisco Catalyst Service Modules related to firewall, VPN, and IPS
- Cisco IPS appliances and various service modules for routers and ASA devices

For a complete list of devices and OS versions supported by Cisco Security Manager, see *Supported Devices and Software Versions for Cisco Security Manager* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

The high-performance and easy-to-use integrated event viewer allows you to centrally monitor events from IPS, ASA, and FWSM devices and correlate them to the related configuration policies. This helps identify problems and troubleshoot configurations. Then, using Configuration Manager, you can make adjustments to the configurations and deploy them. Event Viewer supports event management for Cisco ASA, IPS, and FWSM devices.

In addition to the Primary Event Data Store, events can be copied and stored in the Extended Event Data Store. The Extended Event Data Store can be used to back up and archive a larger number of events. This is useful for historical review and analysis of events where Event Viewer can gather event data from both the Primary Event Data Store and the Extended Event Data Store. The Extended Event Data Store can be enabled in Event Management in Security Manager's Administration settings.

For supported platforms and more information, see the “Monitoring and Diagnostics” section of the *User Guide for Cisco Security Manager 4.1* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

The new integrated report management allows you to generate and schedule ASA, IPS, and remote access VPN reports. Reports for ASA and IPS devices are created by aggregating and summarizing events collected by the Event Viewer. Security reports can be used to efficiently monitor, track, and audit network use and security problems reported by managed devices. Report Manager helps in developing and customizing reports for Cisco ASA and IPS devices.

For supported platforms and more information, see the “Monitoring and Diagnostics” part of the *User Guide for Cisco Security Manager 4.1* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

Table 5-24 PCI Assessment Summary—Cisco Security Manager

Models Assessed
Cisco Security Manager version 4.0.1

Table 5-24 PCI Assessment Summary—Cisco Security Manager (continued)

PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary function of Cisco Security Manager is to implement security configuration in firewalls, routers, and intrusion detection devices based on policy templates to secure the cardholder data environment. (1.2) Table 5-24 lists the component assessment details for Cisco Security Manager.

Table 5-25 Component Capability Assessment—Cisco Security Manager

Cisco Security Manager	
PRIMARY FUNCTION	Requirement 1 (1.2)
Implement security configuration based on policy templates to secure the cardholder data environment.	
CAPABILITY	ASSESSMENT
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- Use descriptive notes for each rule set. These are displayed as remarks in the running configuration.
- Virtualize firewall rule set deployment by using a consistent interface naming standard.
- Apply the anti-spoofing feature to all interfaces using FlexConfig.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are no unnecessary services enabled by default Cisco Security Manager. Cisco Security Manager should be installed on a hardened operating system.

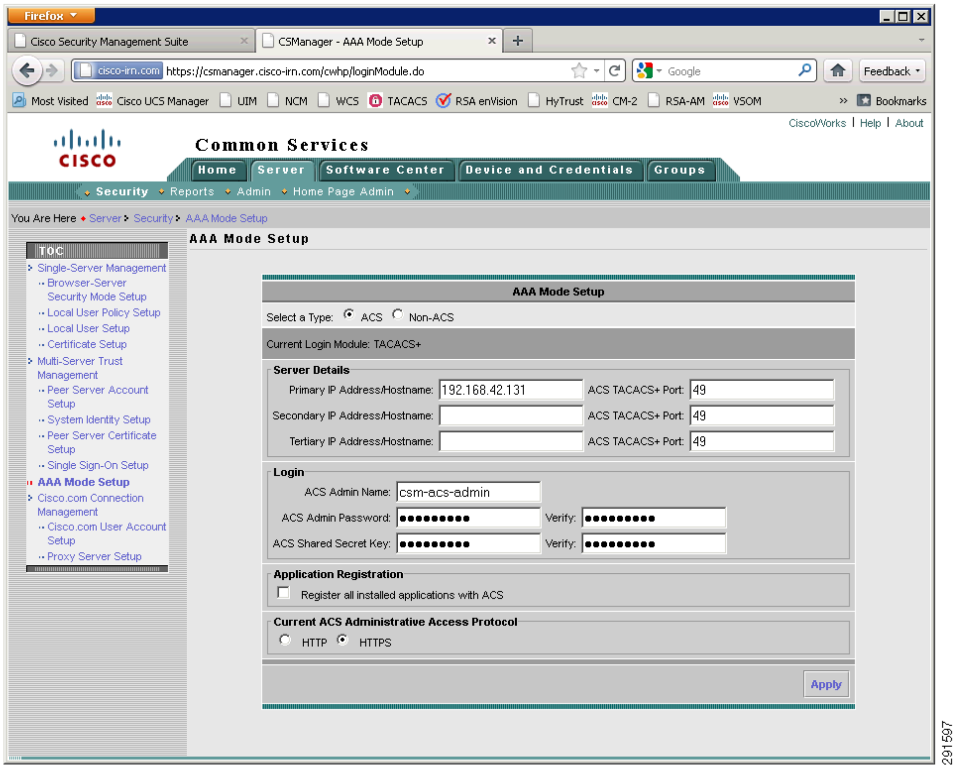
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Security Manager should be installed on a hardened operating system.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Figure 5-67 shows how the Cisco Security Manager is configured in Common Services for ensuring that only encrypted communications for administration are used.

Figure 5-67 CSM Secure Administration and AAA Policy



AAA Mode Setup

Select a Type: ● ACS ○ Non-ACS

Current Login Module: TACACS+

Server Details

Primary IP Address/Hostname:	192.168.42.131	ACS TACACS+ Port:	49
Secondary IP Address/Hostname:		ACS TACACS+ Port:	49
Tertiary IP Address/Hostname:		ACS TACACS+ Port:	49

Login

ACS Admin Name:	csm-acs-admin		
ACS Admin Password:	●●●●●●●●●	Verify:	●●●●●●●●●●
ACS Shared Secret Key:	●●●●●●●●●	Verify:	●●●●●●●●●●

Application Registration

□ Register all installed applications with ACS

Current ACS Administrative Access Protocol

○ HTTP ● HTTPS

Apply

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Security Manager. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Figure 5-67 shows that Cisco Security Manager AAA role setup type was implemented as Cisco Secure ACS, and identified the appropriate Cisco Secure ACS servers.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

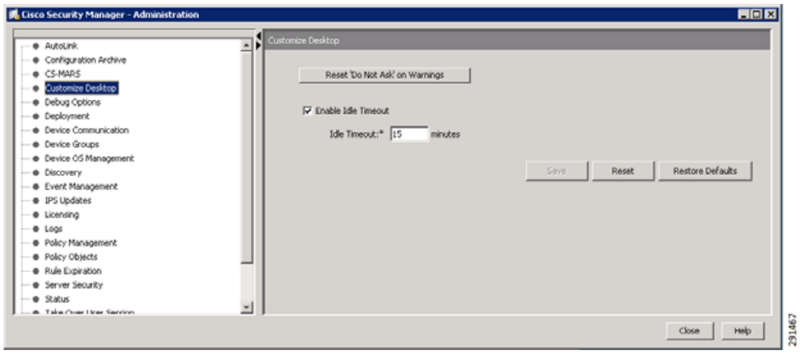
Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

Figure 5-68 shows the configuration setting in the client for setting the idle timeout.

Figure 5-68 Customize Desktop



Cisco Security Manager - Administration

Customize Desktop

☑ Enable Idle Timeout

Idle Timeout:* 15 minutes

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Security Manager is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*

- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Security Manager uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

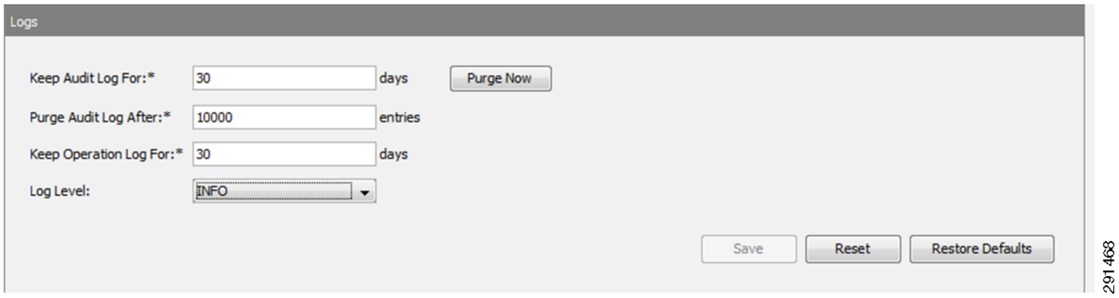
  Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

Figure 5-69, Figure 5-70, and Figure 5-71 shows the Logs, Audit Report, and View Settings screens.

Figure 5-69 Logs



Logs

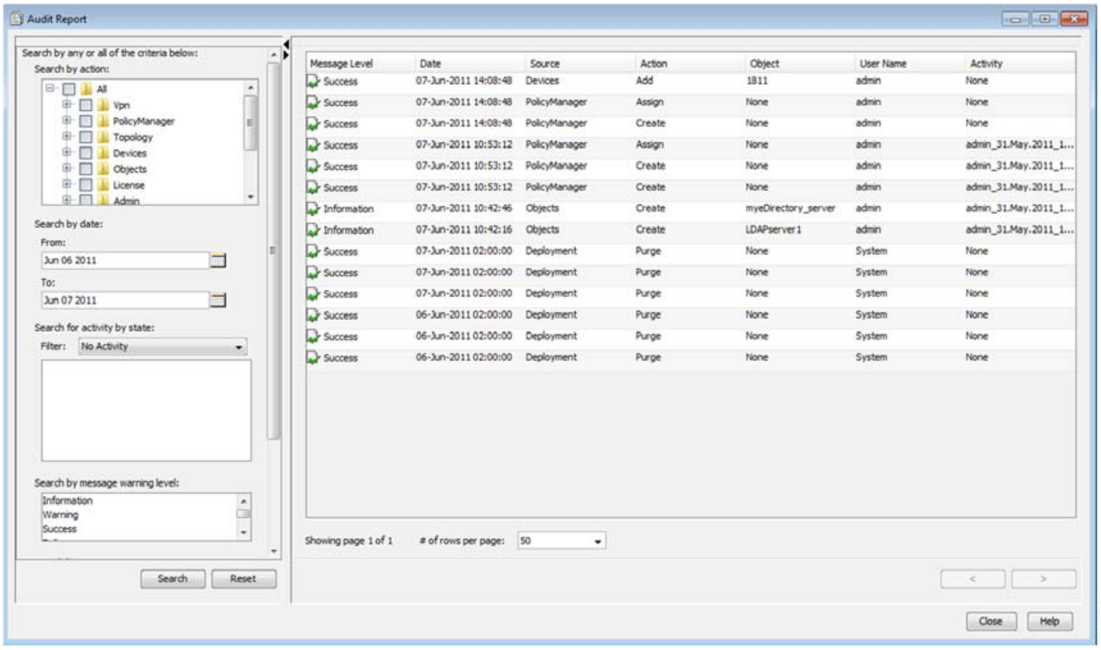
Keep Audit Log For:* 30 days

Purge Audit Log After:* 10000 entries

Keep Operation Log For:* 30 days

Log Level: INFO

Figure 5-70 Audit Report



Audit Report

Search by any or all of the criteria below:

Search by action:

- □ All
  - □ Vpn
  - □ PolicyManager
  - □ Topology
  - □ Devices
  - □ Objects
  - □ License
  - □ Admin

Search by date:

From: Jun 06 2011

To: Jun 07 2011

Search for activity by state:

Filter: No Activity

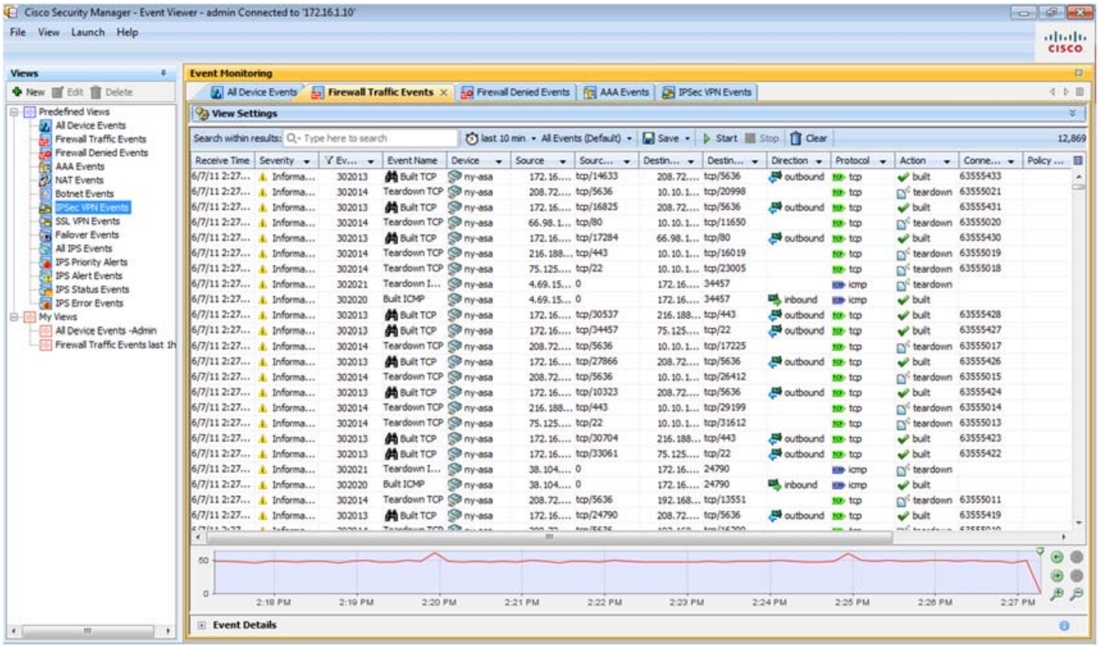
Search by message warning level:

Information
Warning
Success

Message Level	Date	Source	Action	Object	User Name	Activity
Success	07-Jun-2011 14:08:48	Devices	Add	1811	admin	None
Success	07-Jun-2011 14:08:48	PolicyManager	Assign	None	admin	None
Success	07-Jun-2011 14:08:48	PolicyManager	Create	None	admin	None
Success	07-Jun-2011 10:53:12	PolicyManager	Assign	None	admin	admin_31.May.2011_1...
Success	07-Jun-2011 10:53:12	PolicyManager	Create	None	admin	admin_31.May.2011_1...
Success	07-Jun-2011 10:53:12	PolicyManager	Create	None	admin	admin_31.May.2011_1...
Information	07-Jun-2011 10:42:46	Objects	Create	myeDirectory_server	admin	admin_31.May.2011_1...
Information	07-Jun-2011 10:42:16	Objects	Create	LDAPserver1	admin	admin_31.May.2011_1...
Success	07-Jun-2011 02:00:00	Deployment	Purge	None	System	None
Success	07-Jun-2011 02:00:00	Deployment	Purge	None	System	None
Success	07-Jun-2011 02:00:00	Deployment	Purge	None	System	None
Success	06-Jun-2011 02:00:00	Deployment	Purge	None	System	None
Success	06-Jun-2011 02:00:00	Deployment	Purge	None	System	None
Success	06-Jun-2011 02:00:00	Deployment	Purge	None	System	None

Showing page 1 of 1 # of rows per page: 50

Figure 5-71 View Settings



Cisco Security Manager - Event Viewer - admin Connected to '172.16.1.10'

- Predefined Views
  - All Device Events
  - Firewall Traffic Events
  - Firewall Denied Events
  - AAA Events
  - NAT Events
  - Botnet Events
  - IPSec VPN Events
  - SSL VPN Events
  - Failover Events
  - All IPS Events
  - IPS Priority Alerts
  - IPS Alert Events
  - IPS Status Events
  - IPS Error Events
- My Views
  - All Device Events -Admin
  - Firewall Traffic Events last 1h

Search within results: Type here to search | last 10 min | All Events (Default)

12,869

Receive Time	Severity	Ev...	Event Name	Device	Source	Sourc...	Destin...	Destin...	Direction	Protocol	Action	Conne...	Policy ...
6/7/11 2:27...	Informa...	302013	Built TCP	ny-asa	172.16....	tcp/14633	208.72....	tcp/5636	outbound	tcp	built	63555433	
6/7/11 2:27...	Informa...	302014	Teardown TCP	ny-asa	208.72....	tcp/5636	10.10.1...	tcp/20998		tcp	teardown	63555021	
6/7/11 2:27...	Informa...	302013	Built TCP	ny-asa	172.16....	tcp/16825	208.72....	tcp/5636	outbound	tcp	built	63555431	
6/7/11 2:27...	Informa...	302014	Teardown TCP	ny-asa	66.98.1...	tcp/80	10.10.1...	tcp/11650		tcp	teardown	63555020	
6/7/11 2:27...	Informa...	302013	Built TCP	ny-asa	172.16....	tcp/17284	66.98.1...	tcp/80	outbound	tcp	built	63555430	
6/7/11 2:27...	Informa...	302014	Teardown TCP	ny-asa	216.188...	tcp/443	10.10.1...	tcp/16019		tcp	teardown	63555019	
6/7/11 2:27...	Informa...	302014	Teardown TCP	ny-asa	75.125....	tcp/22	10.10.1...	tcp/23005		tcp	teardown	63555018	
6/7/11 2:27...	Informa...	302021	Teardown I...	ny-asa	4.69.15...	0	172.16....	34457		icmp	teardown		
6/7/11 2:27...	Informa...	302020	Built ICMP	ny-asa	4.69.15...	0	172.16....	34457	inbound	icmp	built		
6/7/11 2:27...	Informa...	302013	Built TCP	ny-asa	172.16....	tcp/30537	216.188...	tcp/443	outbound	tcp	built	63555428	
6/7/11 2:27...	Informa...	302013	Built TCP	ny-asa	172.16....	tcp/34457	75.125....	tcp/22	outbound	tcp	built	63555427	
6/7/11 2:27...	Informa...	302014	Teardown TCP	ny-asa	208.72....	tcp/5636	10.10.1...	tcp/17225		tcp	teardown	63555017	
6/7/11 2:27...	Informa...	302013	Built TCP	ny-asa	172.16....	tcp/27866	208.72....	tcp/5636	outbound	tcp	built	63555426	
6/7/11 2:27...	Informa...	302014	Teardown TCP	ny-asa	208.72....	tcp/5636	10.10.1...	tcp/26412		tcp	teardown	63555015	
6/7/11 2:27...	Informa...	302013	Built TCP	ny-asa	172.16....	tcp/10323	208.72....	tcp/5636	outbound	tcp	built	63555424	
6/7/11 2:27...	Informa...	302014	Teardown TCP	ny-asa	216.188...	tcp/443	10.10.1...	tcp/29199		tcp	teardown	63555014	
6/7/11 2:27...	Informa...	302014	Teardown TCP	ny-asa	75.125....	tcp/22	10.10.1...	tcp/31612		tcp	teardown	63555013	
6/7/11 2:27...	Informa...	302013	Built TCP	ny-asa	172.16....	tcp/30704	216.188...	tcp/443	outbound	tcp	built	63555423	
6/7/11 2:27...	Informa...	302013	Built TCP	ny-asa	172.16....	tcp/33061	75.125....	tcp/22	outbound	tcp	built	63555422	
6/7/11 2:27...	Informa...	302021	Teardown I...	ny-asa	38.104....	0	172.16....	24790		icmp	teardown		
6/7/11 2:27...	Informa...	302020	Built ICMP	ny-asa	38.104....	0	172.16....	24790	inbound	icmp	built		
6/7/11 2:27...	Informa...	302014	Teardown TCP	ny-asa	208.72....	tcp/5636	192.168...	tcp/13551		tcp	teardown	63555011	
6/7/11 2:27...	Informa...	302013	Built TCP	ny-asa	172.16....	tcp/24790	208.72....	tcp/5636	outbound	tcp	built	63555419	

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

EMC Ionix Network Configuration Manager

EMC Ionix Network Configuration Manager is a model-based, automated network compliance, change, and configuration management product. It delivers features, advantages, and benefits that ensure the compliance, operational efficiency, security, and availability of your network.

Ionix Network Configuration Manager supplies industry-recognized best practices, enhancing collaborative network infrastructure design, verifying controlled change processes, providing network device and service configuration transparency, and ensuring compliance with corporate and regulatory requirements.

Table 5-26 PCI Assessment Summary—EMC Ionix NCM

Models Assessed	
EMC Ionix Network Configuration Manager version 4.1.0.863 HF7	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary function is to manage network device configuration and verify configuration against policy templates.

Table 5-26 lists the component assessment details for EMC Ionix Network Configuration Manager.

Table 5-27 Component Capability Assessment—EMC Ionix NCM

EMC Ionix NCM	
PRIMARY FUNCTION	**Requirement 1**
Manage network device configuration and verify configuration against policy templates.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

No specific design considerations apply when implementing EMC Ionix NCM.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  Cisco SMARTnet services provide ongoing access to software updates and security patches.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

EMC Ionix Network Configuration Manager is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*
- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

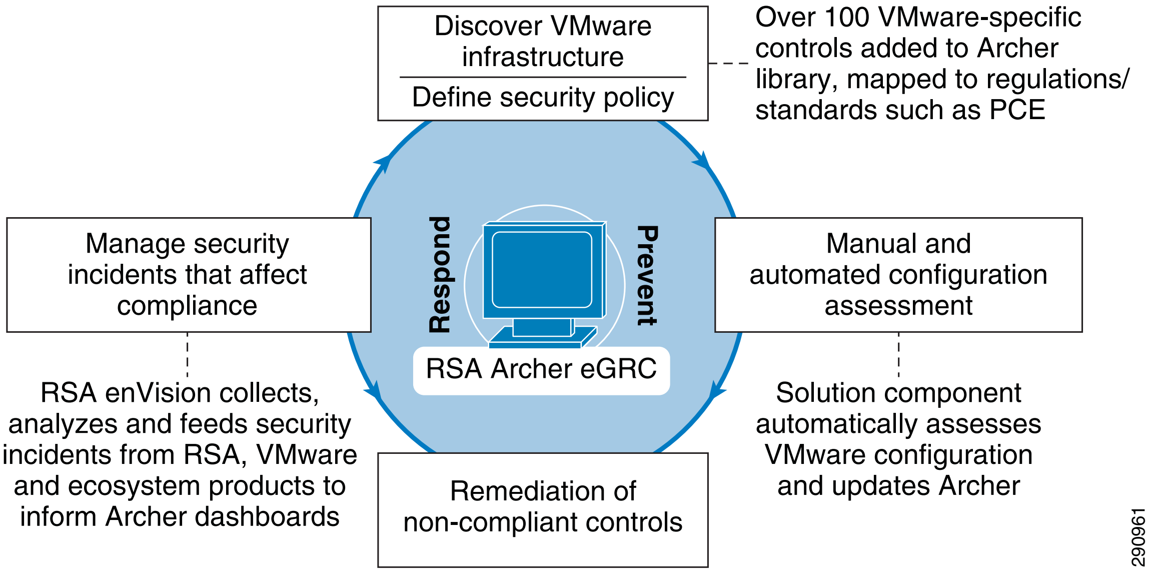
RSA Archer

The RSA Archer eGRC Suite for enterprise governance, risk, and compliance allows your organization to jumpstart your PCI compliance program by conducting continuous, automated assessments to gain the visibility you need to manage and mitigate risk.

Note RSA Archer was initially reviewed by Verizon Business and determined to be outside the scope of the PCI Audit. RSA Archer does store, process, or transmit sensitive cardholder data. There are no Assessment Summary or Capability Assessment details for this product.

RSA Archer provides a comprehensive library of policies, control standards, procedures, and assessments mapped to PCI DSS and other regulatory standards. RSA Archer is designed to orchestrate and visualize the security of both VMware virtualization infrastructure and physical infrastructure from a single console. (See Figure 5-72.)

Figure 5-72 Using Firewall and IDS/IPS


Discover VMware infrastructure
Define security policy
Over 100 VMware-specific controls added to Archer library, mapped to regulations/ standards such as PCE
Manage security incidents that affect compliance
Respond
Prevent
RSA Archer eGRC
Manual and automated configuration assessment
RSA enVision collects, analyzes and feeds security incidents from RSA, VMware and ecosystem products to inform Archer dashboards
Remediation of non-compliant controls
Solution component automatically assesses VMware configuration and updates Archer
290961

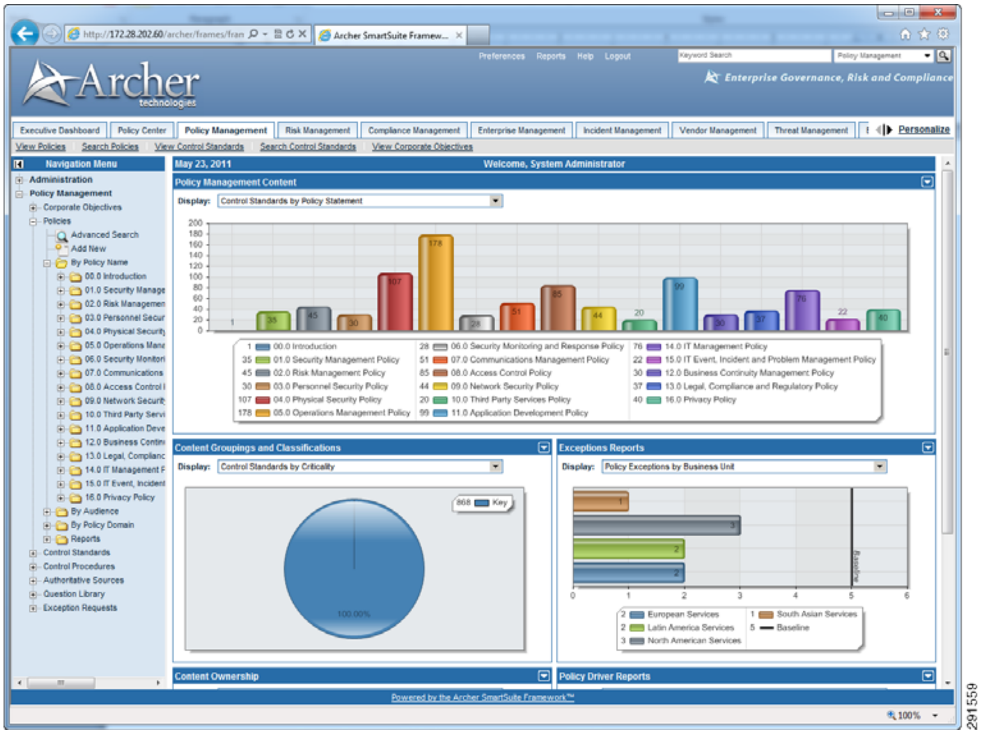
One of the major changes to PCI DSS 2.0 is its clarification on the use of virtualization technology in the cardholder data environment. If virtualization technology is used, the virtualization platform is always in scope for PCI. More than 130 control procedures in the Archer library have been written specifically for VMWare environments and have been mapped to PCI requirements. The RSA Cloud Security and Compliance solution includes software that substantially automates the assessment of whether VMware security controls have been implemented correctly. The results of these automated configuration checks are fed directly into the RSA Archer eGRC Platform, which also captures the results of configuration checks for physical assets via pre-built integration with commercially available scan technologies.

Although a significant number of the VMware control procedures are tested automatically, the remainder must be tested manually because their status cannot be directly inferred from the environment. For these control procedures, project managers can issue manual assessments from the RSA Archer eGRC Platform, using a pre-loaded bank of questions. Project managers can create new questionnaires within minutes and issue them to appropriate users based on asset ownership. Those users are automatically notified of their assessments via rules-driven workflow and My Tasks lists, and can complete their assessments online.

Results for both automated and manual assessments are consolidated in the RSA Archer eGRC Platform and mapped to PCI DSS and other regulations and standards. IT and security operations teams can then monitor compliance with regulations and internal policies across the physical and virtual infrastructure by device, policy, procedure, regulation, and other criteria. This information is presented through a graphical dashboard view, making the information easy to digest and understand.

Configuring the physical and virtual infrastructure according to best-practice security guidelines and regulatory requirements is critical. However, the security and compliance process does not stop there. Organizations also require the ability to monitor misconfigurations, policy violations, and control failures across their infrastructure; and to respond swiftly with appropriate remediation steps. Deficiencies identified through automated and manual configuration checks are captured within the RSA Archer eGRC Platform for management. Control failures are then assigned to appropriate personnel, who can respond by completing remediation tasks or logging exception requests that identify effective compensating controls and are tracked in a Policy Management dashboard, as shown in Figure 5-73.

Figure 5-73 RSA Archer Policy Management



Display: Control Standards by Policy Statement

Display: Control Standards by Criticality

Display: Policy Exceptions by Business Unit

Encryption

A subtle, yet potentially significant change to key management has been introduced with the PCI 2.0 standard. With past versions of the DSS, annual key rotations were required for encryption keys. PCI DSS 2.0 now requires that keys are rotated at the end of their *cryptoperiod*, and references the NIST 800-57 Special Publication to determine what an appropriate cryptoperiod is. The NIST 800-57 Special Publication is a 324-page, three-part document. Merchants, and even QSAs, may not have the expertise to fully understand such a document that includes countless encryption scenarios, with cryptoperiods ranging from as short as a day and as long as three years.

In an ideal world, with all parties being expert cryptographers, this risk-based change to the standard would be very appropriate and most welcome. However, given the number of scenarios and criteria for determining an appropriate cryptoperiod, it could suggest that this change is too subjective and may become a point of contention between a merchant and QSA assessor, as to what is an appropriate cryptoperiod, whereas the former, more prescriptive control, did not allow for flexibility in this area.

RSA Data Protection Manager

RSA Data Protection Manager (formerly RSA Key Manager) provides encryption, tokenization, and key management capabilities. It can be used to achieve PCI Requirement 3 compliance for protecting stored cardholder data, regardless of where the information resides.

RSA Data Protection Manager is an easy-to-use management tool for encrypting keys at the database, file server, and storage layers. It is designed to lower the total cost of ownership and simplify the deployment of encryption throughout the enterprise. It also helps ensure that information is properly secured and fully accessible when needed at any point in its lifecycle through a powerful management console and built-in high availability features. RSA Data Protection Manager provides a comprehensive platform for enforcing and managing the security of sensitive data.

Table 5-28 PCI Assessment Summary—RSA Data Protection Manager

Models Assessed	
RSA Data Protection Manager	version KM-3.1 / AM-6.1.SP3
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of RSA Data Protection Manager is to securely manage the keys that protect cardholder data. (3.5)

Table 5-28 lists the component assessment details for RSA Data Protection Manager.

Table 5-29 Component Capability Assessment—RSA Data Protection Manager

RSA Data Protection Manager	
PRIMARY FUNCTION	**Requirement 3 (3.5)**
Securely manages the keys that protect cardholder data.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

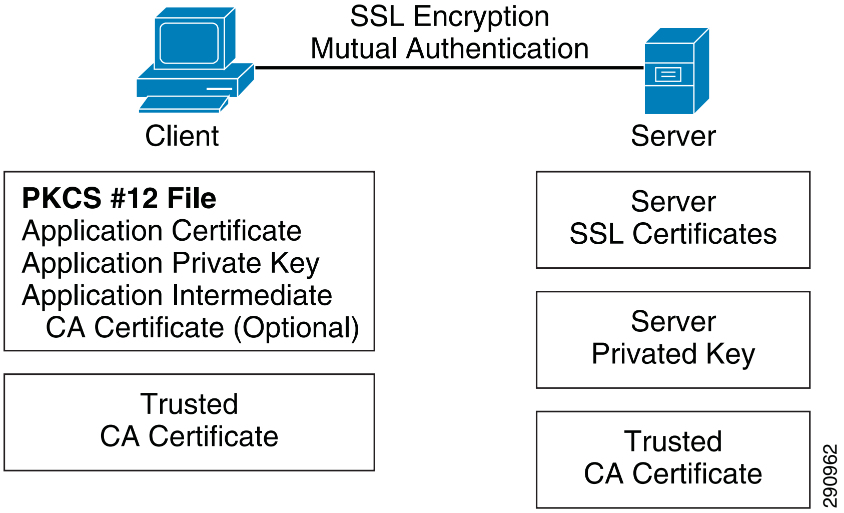
RSA Data Protection Manager's encryption and key management capabilities can be used to store the data in a compliant manner. RSA Data Protection Manager provides application development libraries that support a wide range of development languages and enables developers to easily integrate encryption into point-of-sale, payment, CRM, ERP, and other business applications that create or process sensitive information. RSA Data Protection Manager can also be used to encrypt data as it flows to both disk and tape by providing key management services to Cisco MDS or EMC storage systems.

Because there were no card handling applications in the simulated lab environment, RSA Data Protection Manager was integrated with Cisco MDS to encrypt all data in the environment regardless of whether it was cardholder data or not.

Public Key Infrastructure (PKI) Requirements

In an RSA Data Protection Manager deployment, a PKI needs to be set up to enable secure communication between the RSA Data Protection server and its clients. (See Figure 5-74.)

Figure 5-74 RSA Data Protection Manager Deployment



The certificates and credentials that need to be prepared include:

- Client PKCS#12 certificate and key pair—Used to authenticate RSA Data Protection Manager clients to the RSA Data Protection Server
- Server SSL certificate and key pair—Used by RSA Data Protection Manager Clients to authenticate the server
- Trusted CA certificate—Installed on both clients and the server to verify the signature of certificates sent by a peer. For example, a RSA Key Manager Client has a trusted CA certificate to verify the signature of the Server certificate.
- Middle CA certificate (optional)—If a certificate is not signed directly by a trusted CA certificate, a middle CA certificate should be installed and sent during SSL connection to verify the certificate chain.

Security Recommendation

Because of vulnerabilities with RSA signatures with a small public exponent, especially 3, RSA recommends that an exponent of F4 (216+1) be used.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The appliance version of RSA Data Protection Manager comes pre-hardened. The software version must be installed into a hardened operating system, application server, and database server.

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The appliance version of RSA Data Protection Manager comes pre-hardened. The software version must be installed into a hardened operating system, application server, and database server.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  RSA Data Protection Manager administrative interfaces are protected using SSL.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  RSA Data Protection Manager publishes security patches at RSA Secure Care Online (https://knowledge.rsasecurity.com/) in accordance with industry best practices to manage and respond to security vulnerabilities to minimize customers' risk of exposure.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the included RSA Access Manager Internal Database. Within RSA Data Protection Manager (and the included Access Manager), individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

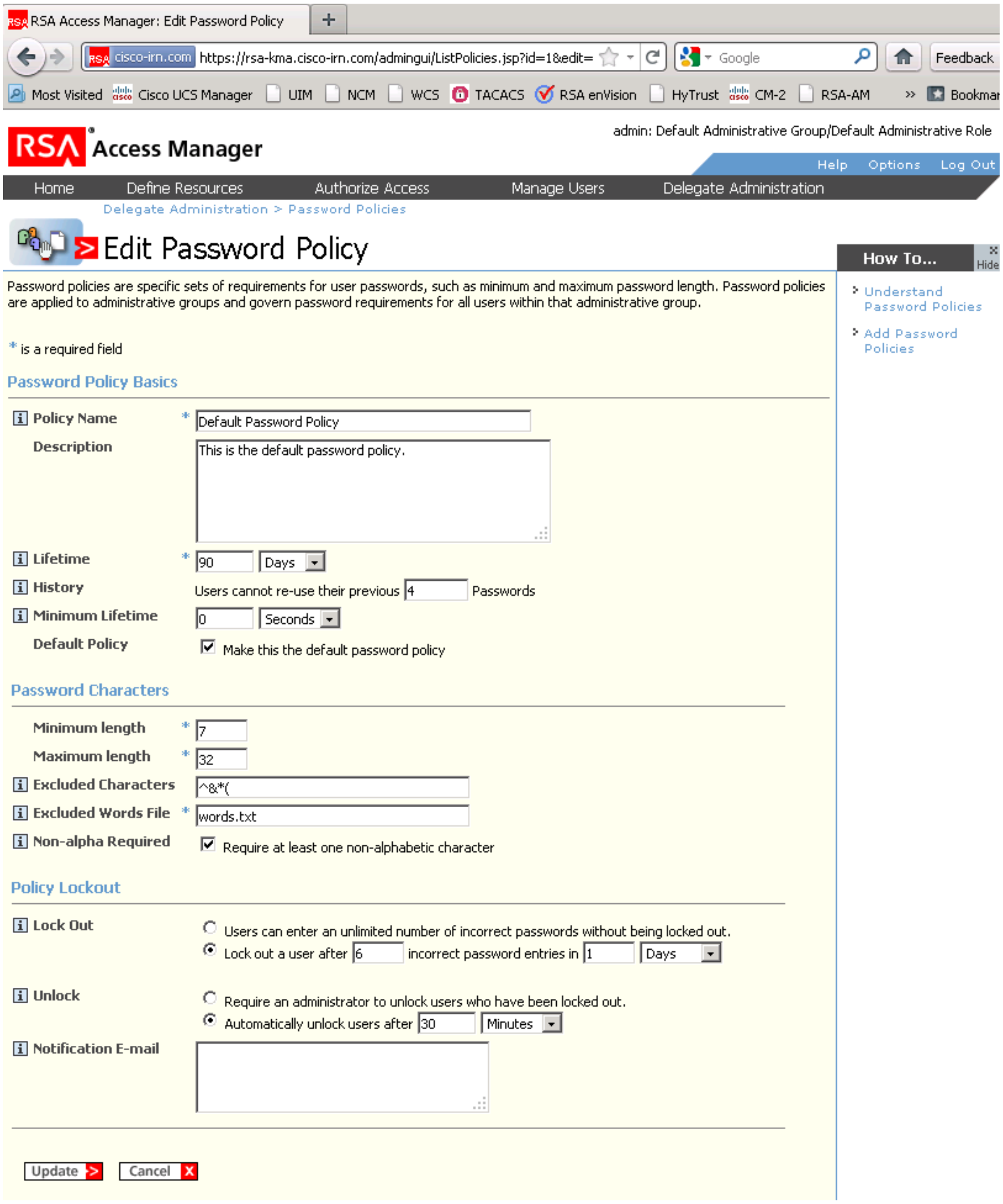
- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  RSA Data Protection Manager embeds and is protected by RSA Access Manager, which has very powerful and flexible capabilities to define password and account lockout policies that can meet all of the above criteria.

  Configuration of user policies is performed via the administration console that can be accessed at the following URL: https://<server address>/admingui/Login.jsp.

  Figure 5-75 shows an appropriate password policy for PCI compliance.

Figure 5-75 Password Policy Settings



admin: Default Administrative Group/Default Administrative Role

Delegate Administration > Password Policies

Edit Password Policy

Password policies are specific sets of requirements for user passwords, such as minimum and maximum password length. Password policies are applied to administrative groups and govern password requirements for all users within that administrative group.

* is a required field

Password Policy Basics

Policy Name * Default Password Policy

Description: This is the default password policy.

Lifetime * 90 Days

History: Users cannot re-use their previous 4 Passwords

Minimum Lifetime: 0 Seconds

Default Policy: ☑ Make this the default password policy

Password Characters

Minimum length * 7

Maximum length * 32

Excluded Characters: ^&*(

Excluded Words File * words.txt

Non-alpha Required: ☑ Require at least one non-alphabetic character

Policy Lockout

Lock Out:
○ Users can enter an unlimited number of incorrect passwords without being locked out.
● Lock out a user after 6 incorrect password entries in 1 Days

Unlock:
○ Require an administrator to unlock users who have been locked out.
● Automatically unlock users after 30 Minutes

Notification E-mail

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database, as shown below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  RSA Data Protection Manager supports the creation of local users. Through company policy, each user must be assigned a unique ID.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts in RSA Data Protection Manager require the setting of a password according to the assigned password policy
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Through company policy, inactive users should be removed or disabled every 90 days. RSA Data Protection Manager also enables setting of an account expiration date for individual accounts.
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  The Default Password policy can be configured to force users to change their passwords every 90 days, as shown in Figure 5-75.
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The Default Password policy can be configured to require a minimum of 7 characters, as shown in Figure 5-75.
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The Default Password policy can be configured require at least one non-alphabetic character by checking the "Non-Alpha Required" box, as shown in Figure 5-75.
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  The Default Password policy can be configured to prevent the re-use of previous passwords by specifying the history number, as shown in Figure 5-75.
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  The Default Password policy can be configured to lock out accounts after a specified number of login failures, as shown in Figure 5-75.
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  The Default Password policy can be configured to lock out accounts for a specified duration or until the administrator re-enables the user ID, as shown in Figure 5-75.
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  RSA Data Protection Manager automatically closes sessions to the administrative consoles after 15 minutes of inactivity.

  RSA Data Protection Manager embeds and is protected by RSA Access Manager, which has very powerful and flexible capabilities to define password and account lockout policies that can meet all of the above criteria.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

RSA Data Protection Manager is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

RSA Data Protection Manager uses Network Time Protocol (NTP) to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. The appliance uses NTP to meet these requirements by specifying the appropriate NTP servers during the installation steps. If NTP servers need to be modified, use the following steps:

1. Open the /etc/ntp.conf file.
2. Under the List Servers section, provide the ntp server ip address or host name to the server parameter.
3. Save the /etc/ntp.conf file.
4. Execute the following commands (as root) to forcibly synchronize the clock of the appliance to the NTP server:

a. Stop the NTPD daemon by typing the following:

```
service ntpd stop
```

b. Execute the following command at least three times (to minimize the offset):

```
ntpdate -u <ntpserver>
```

c. Start the NTPD daemon by typing the following:

```
service ntpd start
```

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*

  Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  RSA Data Protection Manager can be configured to send its log data to the RSA enVision log management platform to meet the above requirements. The configuration procedure is documented in the enVision Event Source Configuration Guide for RSA Data Protection Manager, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/)

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Storage

EMC SAN Disk Array

The EMC SAN disk array is used to securely store sensitive compliance data within the data center. Using virtual storage technology, retailers are able to safely combine (in-scope) sensitive date with (out-of-scope) data while maintaining the compliance boundary.

EMC technology combines midrange networked storage with innovative technology and robust software capabilities to manage and consolidate your data.

Table 5-30 PCI Assessment Summary—EMC SAN Disk Array

Models Assessed	
EMC CLARiiON CX-240 EMC Unified Infrastructure Manager version 2.0.1.1.160	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15

Table 5-30 PCI Assessment Summary—EMC SAN Disk Array (continued)

PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of the EMC SAN disk array is to store cardholder data. There is no direct PCI requirement for this storage function.

Table 5-30 lists the component assessment details for the EMC SAN disk array.

Table 5-31 Component Capability Assessment—EMC SAN Disk Array

EMC SAN Disk Array	
PRIMARY FUNCTION	**Requirement N/A**
Securely store sensitive compliance data within the data center.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

The EMC SAN disk array is a primary component of VCE Vblock architecture. Vblock 1 is designed for medium-to-high numbers of virtual machines, and is ideally suited to a broad range of usage scenarios, including shared services, e-mail, file and print, virtual desktops, and collaboration.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The storage management server provides 256-bit symmetric encryption of all data passed between it and the client components that communicate with it, as listed in the "Port Usage" section (Web browser, Secure CLI), as well as all data passed between storage management servers. The encryption is provided via SSL/TLS and uses the RSA encryption algorithm
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The EMC Storage system does not run any unnecessary services by default.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  When you connect to Unisphere through http://<clariion_ip> (port 80), a Java applet is delivered to the browser on your computer. The applet establishes a secure connection over SSL/TLS (port 443) with the storage management server on the CLARiiON storage system. Therefore, even though "https://" is not displayed in the browser, the connection is secure.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  EMC Powerlink services provide ongoing access to software updates and security patches.

  CLARiiON storage systems do not support installation of third-party utilities or patches. EMC will provide an officially released FLARE Operating Environment patch if needed to correct a security-related issue (or any other kind of issue).

  For information on product updates, see the following URL:
  https://support.emc.com/products/CLARiiONCX4

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by the EMC SAN disk array using LDAP services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*

- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

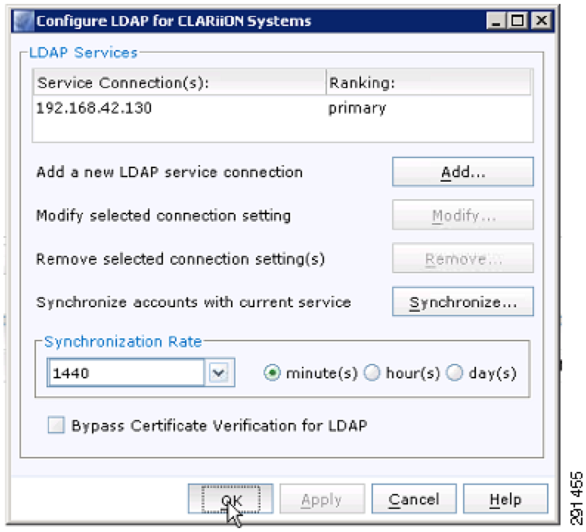
When you start a session, Unisphere prompts you for a username, password, and scope (local, global, or LDAP). These credentials are encrypted and sent to the storage management server. The storage management server then attempts to find a match within the user account information. If a match is found, you are identified as an authenticated user.

LDAP Authentication should be used for PCI compliance because the local authentication does not meet all PCI 8 requirements for secure user access and accounts.

Step 1 To configure LDAP authentication, go to the Domains tab, then select **Configure LDAP for CLARiiON Systems** from the Users menu on the left.

Step 2 Add a new LDAP service by clicking **Add** and then **OK**, as shown in Figure 5-76.

Figure 5-76 Adding LDAP Service



Configure LDAP for CLARiiON Systems

LDAP Services

Service Connection(s):	Ranking:
192.168.42.130	primary

Add a new LDAP service connection

Modify selected connection setting

Remove selected connection setting(s)

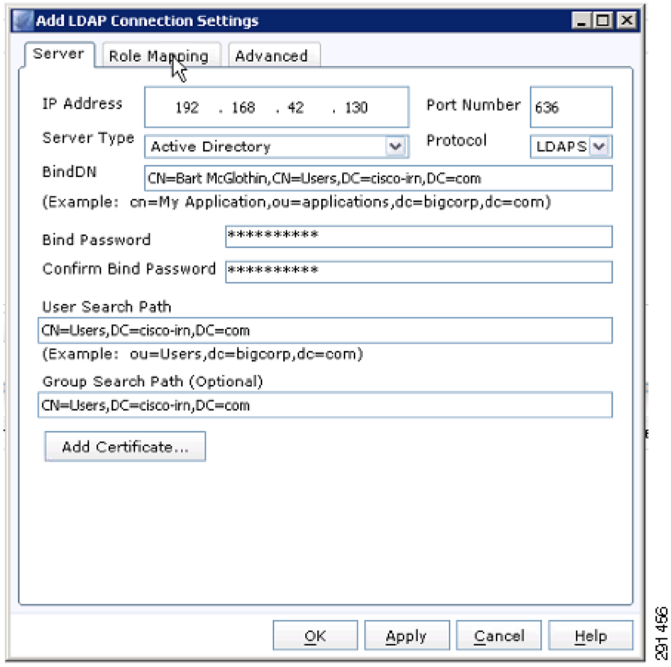
Synchronize accounts with current service

Synchronization Rate: 1440 ● minute(s) ○ hour(s) ○ day(s)

□ Bypass Certificate Verification for LDAP

Step 3 Configure the LDAP server for Active Directory as shown in Figure 5-77.

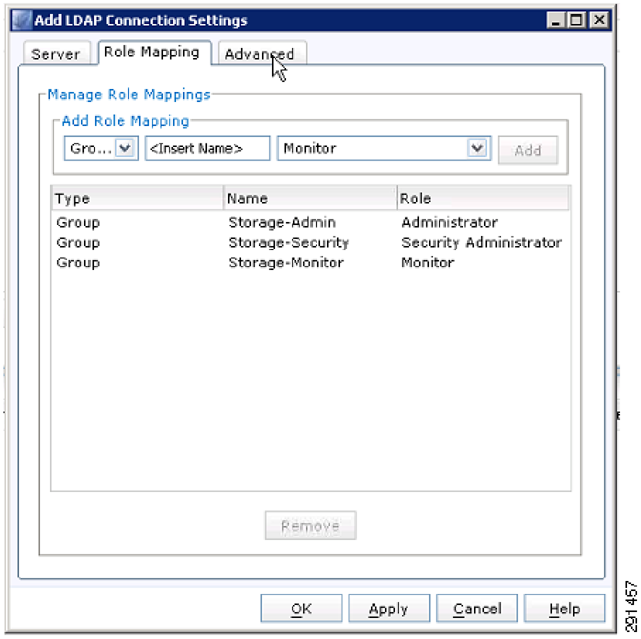
Figure 5-77 Configuring the LDAP Server for Active Directory



IP Address: 192 . 168 . 42 . 130
Port Number: 636
Server Type: Active Directory
Protocol: LDAPS
BindDN: CN=Bart McGlothin,CN=Users,DC=cisco-irn,DC=com
(Example: cn=My Application,ou=applications,dc=bigcorp,dc=com)
Bind Password: **********
Confirm Bind Password: **********
User Search Path: CN=Users,DC=cisco-irn,DC=com
(Example: ou=Users,dc=bigcorp,dc=com)
Group Search Path (Optional): CN=Users,DC=cisco-irn,DC=com

Step 4 After communications are established with the LDAP service, specific LDAP users or groups must be given access to Unisphere by mapping them to Unisphere roles. The LDAP service merely performs the authentication. Once authenticated, user authorization is determined by the assigned Unisphere role. The most flexible configuration is to create LDAP groups that correspond to Unisphere roles. This allows you to control access to Unisphere by managing the members of the LDAP groups. Roles were configured as shown in Figure 5-78.

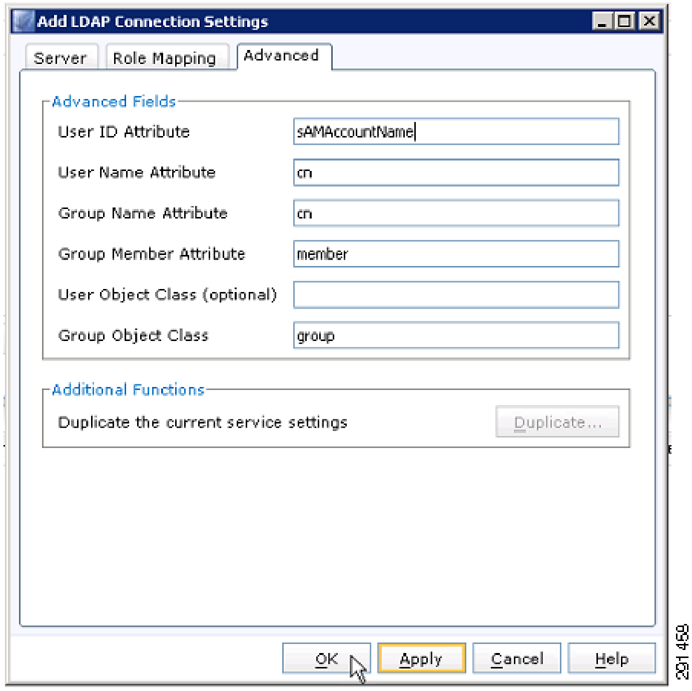
Figure 5-78 Role Mapping



Type	Name	Role
Group	Storage-Admin	Administrator
Group	Storage-Security	Security Administrator
Group	Storage-Monitor	Monitor

Step 5 The Advanced features were left at their default settings, as shown in Figure 5-79.

Figure 5-79 Advanced Settings



Advanced Fields

User ID Attribute sAMAccountName

User Name Attribute cn

Group Name Attribute cn

Group Member Attribute member

User Object Class (optional)

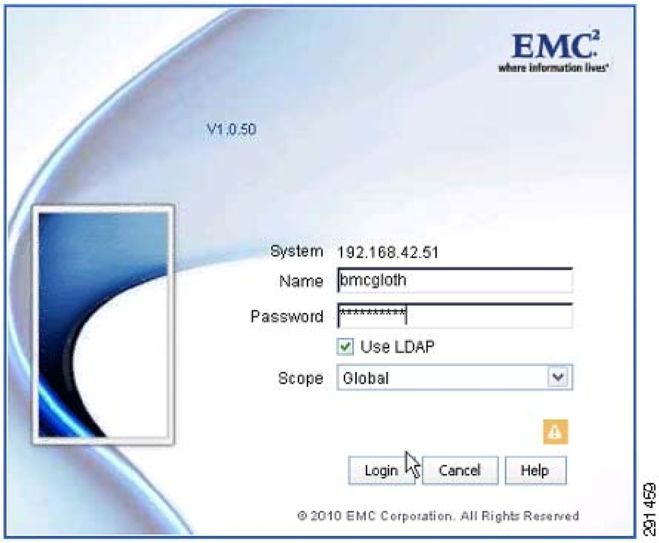
Group Object Class group

Additional Functions

Duplicate the current service settings

Step 6 You can then log out, and log back in, selecting the **Use LDAP** option for centralized authentication, as shown in Figure 5-80.

Figure 5-80 Selecting Use LDAP Function



System 192.168.42.51

Name bmcgloth

Password **********

☑ Use LDAP

Scope Global

© 2010 EMC Corporation. All Rights Reserved

Step 7 For further installation information, see the *FLARE 30 Security Configuration Guide* on EMC Powerlink for configuring LDAP/Active Directory authentication.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the LDAP authentication capabilities to the Windows Active Directory server for AAA services. Microsoft Active Directory contains the necessary user account services for all of the appropriate PCI 8 requirements. Configure AAA services as shown above in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.PCI Sub-Requirements with Compensating Controls*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

EMC CLARiiON is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*

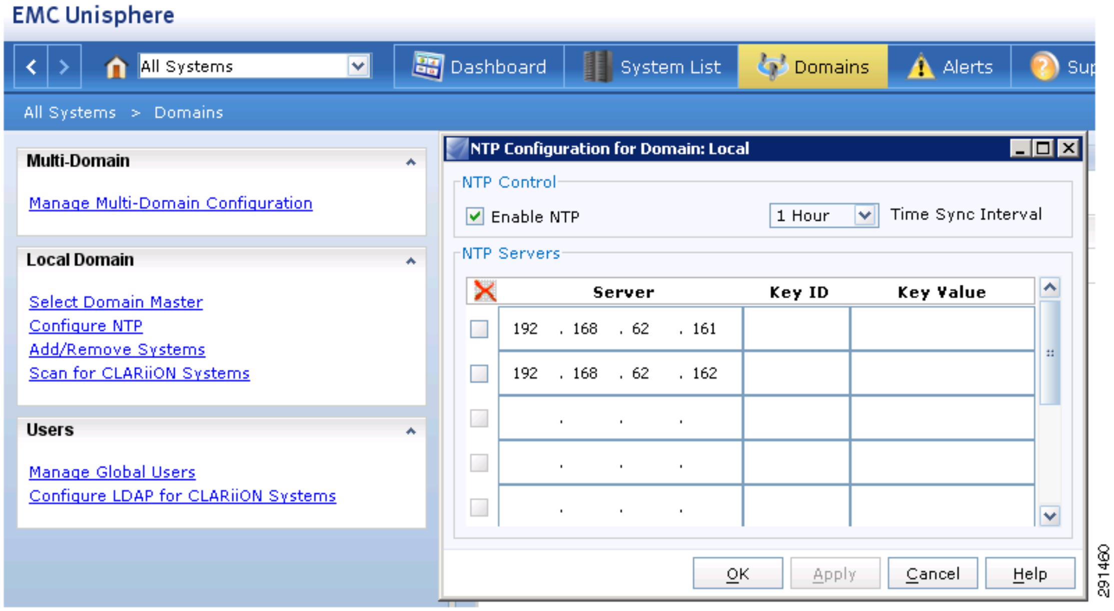
- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

EMC CLARiiON uses Network Time Protocol (NTP) to update and synchronize local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. EMC CLARiion uses NTP to meet these requirements by implementing the configuration statements shown in Figure 5-81.

Figure 5-81 NTP Configuration for Domain: Local



NTP Configuration for Domain: Local

NTP Control

☑ Enable NTP   1 Hour   Time Sync Interval

NTP Servers

	Server	Key ID	Key Value
□	192 . 168 . 62 . 161		
□	192 . 168 . 62 . 162		
□	. . .		
□	. . .		
□	. . .		

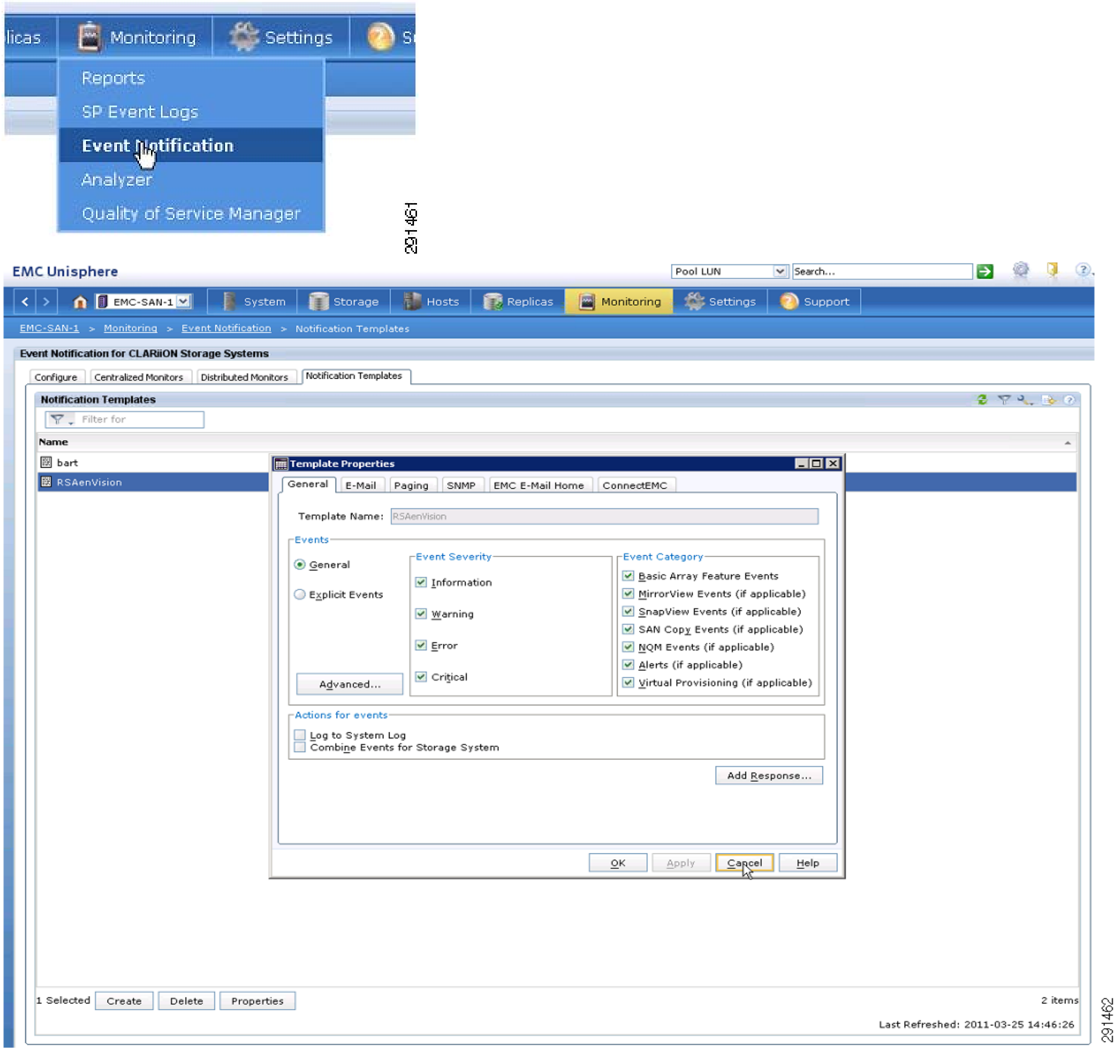
- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

  PCI 10.5.5—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

SP event logs on CLARiiON storage systems can store only a fixed number of events and will wrap if that limit is exceeded. This may take days, weeks, months, or years depending on the logging activity. Therefore, because PCI requires keeping all logs for a set period of time, you need to archive the logs from the CLARiiON storage system on a regular basis. You can do this with the CLI **getlog** command, but a much more integrated method is to use the "log to system log" option of the Event Monitor template to log events to the Windows system log. You can then archive these logs as required.

Additional SNMP Traps are configured to send event notifications directly and immediately to RSA enVision. (See Figure 5-82.)

Figure 5-82 Using Log to System Log Option



Template Name: RSAenVision

Events

● General

○ Explicit Events

Event Severity

☑ Information

☑ Warning

☑ Error

☑ Critical

Event Category

☑ Basic Array Feature Events

☑ MirrorView Events (if applicable)

☑ SnapView Events (if applicable)

☑ SAN Copy Events (if applicable)

☑ NQM Events (if applicable)

☑ Alerts (if applicable)

☑ Virtual Provisioning (if applicable)

Actions for events

□ Log to System Log

□ Combine Events for Storage System

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls—EMC SAN

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Monitoring

RSA enVision

RSA enVision is a security information and event management (SIEM) platform that provides the capability to implement PCI requirement 10 to track and monitor all access to network resources and cardholder data. RSA enVision does this by collecting, permanently archiving, and processing all the log and event data generated by devices and applications within your network, and generating alerts when it observes suspicious patterns of behavior. Administrators can interrogate the full volume of stored data through an intuitive dashboard, and can use advanced analytical software to gain visibility and understanding of how their network is used and the threats and risks to the infrastructure and applications.

The RSA enVision platform can draw logs from tens of thousands of devices at once, including Cisco network devices, the VCE Vblock infrastructure, the VMware virtual environment, Cisco ASA firewalls, Cisco IPS devices, Cisco IronPort E-mail Appliance, other RSA products, and the HyTrust appliance. Out of the box, RSA enVision can produce PCI 2.0 compliance reports and alerts based on the log and event data it collects. RSA enVision also offers powerful tools to create custom reports and alerts specific to your environment.

Table 5-32 PCI Assessment Summary—RSA enVision

Models Assessed	
RSA enVision version 4.0, Revision 5	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of RSA enVision is to securely store and correlate the system logs that is receives. (10.5)

Table 5-32 lists the component assessment details for RSA enVision.

Table 5-33 Component Capability Assessment—RSA enVision

RSA enVision	
PRIMARY FUNCTION	**Requirement 10 (10.5)**
Securely store and correlate the system logs that it receives.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

Depending on the size of your network, RSA enVision may be deployed as a standalone, self-contained, security-hardened appliance or in a distributed deployment to cope with the demands of the largest enterprise networks. When deployed in a distributed architecture, multiple dedicated appliances are deployed where required to perform key roles. Local and remote collectors perform data collection. Data servers manage the data. Application servers perform analysis and reporting. Data itself can be stored using direct attached, online, near-line or offline storage from the full EMC storage portfolio.

RSA enVision does not require any client-side agents to pull log or event data from your infrastructure or applications. RSA enVision can integrate with event sources through standard protocols such as syslog or SNMP by configuring the event source to send data to enVision. For richer event data, enVision integrates with some event sources through their APIs or directly with their database backends. Specific event source device configuration procedures can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/)

RSA enVision is sold as a standalone appliance. It is available in a variety of hardware options based on the requirements of the enterprise design. The system comes pre-installed on an already hardened operation system.

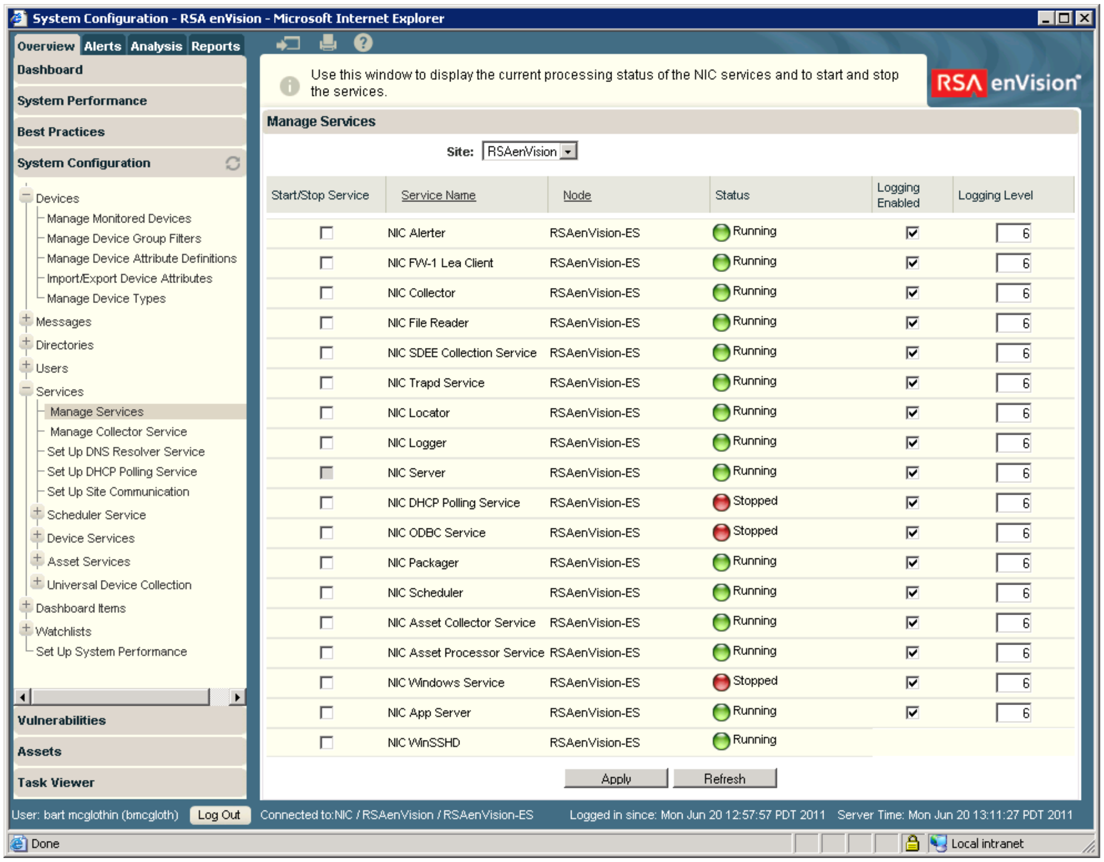
PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  RSA enVision services can be independently enabled or disabled, depending on what protocols are required to collect log and event data, as shown in Figure 5-83.

Figure 5-83 RSA enVision Managed Services



Use this window to display the current processing status of the NIC services and to start and stop the services.

Manage Services

Site: RSAenVision

Start/Stop Service	Service Name	Node	Status	Logging Enabled	Logging Level
☐	NIC Alerter	RSAenVision-ES	Running	☑	6
☐	NIC FW-1 Lea Client	RSAenVision-ES	Running	☑	6
☐	NIC Collector	RSAenVision-ES	Running	☑	6
☐	NIC File Reader	RSAenVision-ES	Running	☑	6
☐	NIC SDEE Collection Service	RSAenVision-ES	Running	☑	6
☐	NIC Trapd Service	RSAenVision-ES	Running	☑	6
☐	NIC Locator	RSAenVision-ES	Running	☑	6
☐	NIC Logger	RSAenVision-ES	Running	☑	6
☐	NIC Server	RSAenVision-ES	Running	☑	6
☐	NIC DHCP Polling Service	RSAenVision-ES	Stopped	☑	6
☐	NIC ODBC Service	RSAenVision-ES	Stopped	☑	6
☐	NIC Packager	RSAenVision-ES	Running	☑	6
☐	NIC Scheduler	RSAenVision-ES	Running	☑	6
☐	NIC Asset Collector Service	RSAenVision-ES	Running	☑	6
☐	NIC Asset Processor Service	RSAenVision-ES	Running	☑	6
☐	NIC Windows Service	RSAenVision-ES	Stopped	☑	6
☐	NIC App Server	RSAenVision-ES	Running	☑	6
☐	NIC WinSSHD	RSAenVision-ES	Running		

User: bart mcglothin (bmcgloth) Connected to:NIC / RSAenVision / RSAenVision-ES Logged in since: Mon Jun 20 12:57:57 PDT 2011 Server Time: Mon Jun 20 13:11:27 PDT 2011

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The RSA enVision appliance ships security-hardened. The embedded Windows 2003 server is hardened to remove all unnecessary functionality.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The RSA enVision web interface is protected using SSL.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  RSA enVision publishes security patches on RSA Secure Care Online (https://knowledge.rsasecurity.com/) in accordance with industry best practices to manage and respond to security vulnerabilities to minimize customers' risk of exposure.

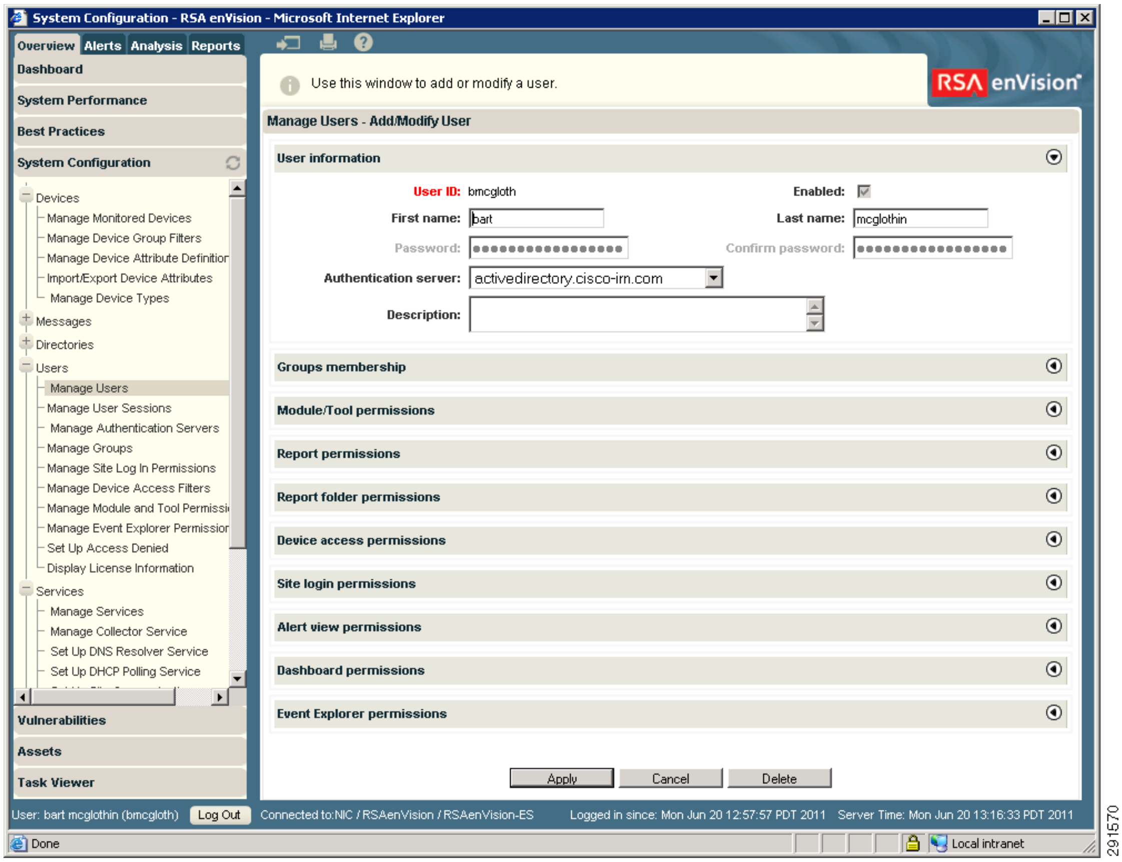
Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 can be met using the RSA enVision Internal Database (as part of its local Windows Active Directory). For validation, RSA enVision was linked to the centralized user database (Active Directory) using LDAP. Within RSA enVision, individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

RSA enVision management interfaces implement role-based access control that can be used to restrict access to privileged user IDs, as shown in Figure 5-84.

Figure 5-84 RSA enVision User Profile



Use this window to add or modify a user.

Manage Users - Add/Modify User

User information

User ID: bmcgloth

Enabled: ☑

First name: bart

Last name: mcglothin

Password: ●●●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●●●

Authentication server: activedirectory.cisco-irn.com

Description:

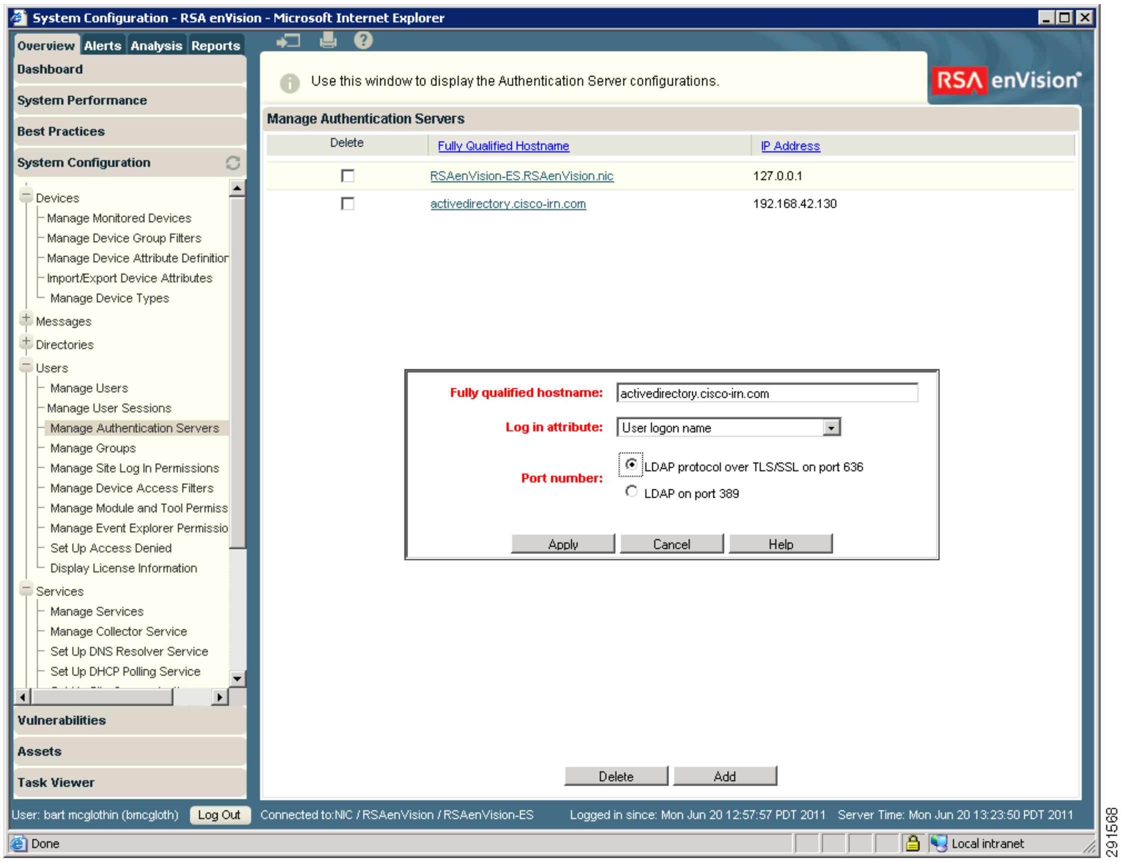
User: bart mcglothin (bmcgloth) Connected to:NIC / RSAenVision / RSAenVision-ES Logged in since: Mon Jun 20 12:57:57 PDT 2011 Server Time: Mon Jun 20 13:16:33 PDT 2011

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

RSA enVision's access control system defaults to deny access.

RSA enVision is configurable to use its local Active Directory database, or an external database via LDAP, as shown in Figure 5-85.

Figure 5-85 RSA enVision Authentication Servers


System Configuration - RSA enVision - Microsoft Internet Explorer
Overview
Alerts
Analysis
Reports
Dashboard
System Performance
Best Practices
System Configuration
Devices
Manage Monitored Devices
Manage Device Group Filters
Manage Device Attribute Definitior
Import/Export Device Attributes
Manage Device Types
Messages
Directories
Users
Manage Users
Manage User Sessions
Manage Authentication Servers
Manage Groups
Manage Site Log In Permissions
Manage Device Access Filters
Manage Module and Tool Permiss
Manage Event Explorer Permissio
Set Up Access Denied
Display License Information
Services
Manage Services
Manage Collector Service
Set Up DNS Resolver Service
Set Up DHCP Polling Service
Vulnerabilities
Assets
Task Viewer
RSA enVision
Apply
Cancel
Help
Delete
Add
Log Out
Done
Local intranet
291568

Use this window to display the Authentication Server configurations.

Manage Authentication Servers

Delete	Fully Qualified Hostname	IP Address
□	RSAenVision-ES.RSAenVision.nic	127.0.0.1
□	activedirectory.cisco-irn.com	192.168.42.130

Fully qualified hostname: activedirectory.cisco-irn.com

Log in attribute: User logon name

Port number: ● LDAP protocol over TLS/SSL on port 636 ○ LDAP on port 389

User: bart mcglothin (bmcgloth) Connected to:NIC / RSAenVision / RSAenVision-ES Logged in since: Mon Jun 20 12:57:57 PDT 2011 Server Time: Mon Jun 20 13:23:50 PDT 2011

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the LDAP authentication capabilities to the Windows Active Directory server for AAA services. Microsoft Active Directory contains the necessary user account services for all of the appropriate PCI 8 requirements. Configure AAA services as shown above in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  RSA enVision can authenticate users against external authentication services such as Windows Active Directory using the LDAP protocol. The above policies can be implemented within Windows Active Directory as was validated in this solution.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

RSA enVision is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

RSA enVision uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4**—*Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  Time synchronization for this windows server is specified through the Domain Policy because the RSA enVision appliance is itself a Domain Controller. The server synchronizes its clock to know time sources using NTP as specified in the initial appliance setup. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*

  Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

  RSA enVision delivers mirrored, unfiltered data to its Internet Protocol Database, which provides the ability to retain data in its original format. Further, "write once, read many" capabilities help ensure that the mirrored copy remains intact, even if the original data is compromised. RSA enVision-captured event logs are stored on a hardened operating system and protected using an integrity check mechanism.

- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*

  RSA enVision's management interfaces implement a role-based access control system to limit who has access to log data.

- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*

  RSA enVision-captured event logs are stored on a hardened operating system in a compressed form and protected via an integrity check mechanism. Access to the operating system and enVision management interfaces can be restricted through operating system and enVision access control systems.

- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

  RSA enVision's primary function is to provide a centralized point for tracking and monitoring access to cardholder data throughout a PCI environment.

- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  RSA enVision stores event data in a tamper evident manner using an internal integrity checking mechanism.

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

HyTrust Appliance

Vblock Infrastructure Platforms from VCE allow retailers to take advantage of the architectural, operational, and financial benefits of virtualization in their PCI infrastructure. HyTrust Appliance (HTA) complements Vblock capabilities by providing:

- Access control for virtual infrastructure including least privilege, separation of duties, and two-factor authentication
- Granular and exhaustive logging and auditing
- Segmentation of infrastructure to support virtualized applications

PCI DSS 2.0 clarifies the use of virtualization technology with the cardholder data environment (CDE) and specifies that the platform is always in scope. This requirement is consistent with additional risks introduced by mobility and the fast-paced change rate of virtualized assets that can now be reconfigured, relocated, and duplicated by remote administrators. These capabilities combined with poor access control create a significant risk. Hypervisor logs geared toward software maintenance and troubleshooting are obviously useful, but not in the context of a compliance audit.

HyTrust Appliance systematically addresses the three broad areas of IT control objectives (access and user administration, change and configuration, and operations), by proactively enforcing policies for all administrative access, regardless of access method: Secure Shell (SSH) to host, VMware vSphere client to host, or VMware vCenter or any of the programmatic access. HyTrust Appliance provides two-factor authentication and role-based access control, logical segmentation of shared infrastructure, root password vaulting, and audit-quality logs of every attempted access.

Table 5-34 PCI Assessment Summary—HyTrust Appliance

Models Assessed	
HyTrust version 2.2.1.14064	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary function of HyTrust Appliance is to provide an automated control and audit facility for the virtual infrastructure and cloud stack. (2, 7, and 10).

Table 5-34 lists the component assessment details for the HyTrust Appliance.

Table 5-35 Component Capability Assessment—HyTrust Appliance

HyTrust Appliance	
PRIMARY FUNCTION	**Requirement 2.3, 7.1, 10.5**
Monitor and secure access to the virtual infrastructure by proxying administrative sessions to VMware vCenter.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

Define rules and deploy policy to activate protection for the virtual infrastructure.

Administrators can define custom rules that restrict entitlement based on specific virtual infrastructure objects that users need to access and manage. Rules that define entitlement can be based on pre-defined roles or administrators can use custom user-defined roles.

The Hytrust appliance provides complete logging of administrator actions by proxying VMware vCenter client connections to the vSphere management server, and clients that try to connect directly to ESX/ESXi hosts. This logging includes the source IP address of the clients, permitted actions and actions that are blocked because the client may not have sufficient privileges (all requirements of PCI that VMware cannot perform natively).

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  HyTrust Appliance configures the virtualization platform (VMware ESX server) to disable unsecure protocols. In addition, HyTrust Appliance proxies non-console management access and redirects attempts to connect via the HTTP management protocol to HTTPS-based connections. In the reference implementation, the configuration of VMware ESX 4.0 servers was performed in accordance with the HyTrust default PCI configuration template. Specifically, the following controls are set:

  ```
  ssh_config: Protocol = 2
  sshd_config:
  Protocol = 2
  X11Forwarding = yes
  IgnoreRhosts = yes
  RhostsAuthentication = no
  RhostsRSAAuthentication = no
  HostbasedAuthentication =no
  PermitRootLogin = no
  PermitEmptyPasswords = no
  Banner = /etc/issue.net if not set
  ```

  Check that a BIOS password is set and that it is not the manufacturer default. For more information, see the following URL: http://www.pwcrack.com/bios.shtml

  Set file permissions on */etc/snmp.conf* and */etc/snmp.conf/preesx* to 700, and set *root* as owner and group.

  Replace the default "COMMUNITY" phrase with a stronger passphrase.

  Restrict SNMP access to authorized IP addresses on a separate admin-network.

  Use read-only mode.

  ```
  - chown root:root & chmod 0600 /etc/security/console.perms or
  /etc/security/console.perms.d/50-default.perms
  - comment out the lines as needed
  - chmod 644 /etc/{profile, pam.d/system_auth, ntp.conf, passwd, group}
  - chmod 600 /etc/ssh/sshd_config
  - chmod 755 /etc/{ntp, vmware}
  - chmod 440 /etc/sudoers
  - chmod 400 /etc/shadow
  ```

  Establish the following local firewall settings:

  ```
  Ports: 22/sshd/inTCP, 53/dns/outUDP, 67-68/dhcp/UDP, 80/http/inTCP, 427/cim slp/TCP,
  443/https/inTCP, 902/vmwareauthd/ inTCP-outTCPUDP, 2050-5000/vmware/TCPUDP,
  5988-89/cim server/inTCP, 27000/license server/outTCP
  ```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  HyTrust Appliance configures the virtualization platform (VMware ESX server) to disable unnecessary boot services. In addition, HyTrust Appliance restricts the use of **sudo** and **su** services and ensures tighter configuration of copy and paste sharing between the host hypervisor and CDE implemented as a virtual system component.

  In addition, HyTrust Appliance periodically monitors the virtualization platform configuration to ensure ongoing compliance with the above sub-requirements.

In the reference implementation, the configuration of VMware ESX 4.0 servers was performed in accordance with the HyTrust default PCI configuration template. Specifically, the following controls were configured and monitored:

All the boot services were disabled on the VMware ESX server except as follows:

```
S00microcode_ctl S00vmkstart S01vmware S02mptctlnode
S08iptables S09firewall S10network S12syslog S13irqbalance
S20random S55sshd S56rawdevices S56xinetd S58ntpd
S85gpm S85vmware-webAccess S90crond S91httpd.vmware
S99local S99pegasus S99vmware-autostart
```

Add following to each VM dot-vmx file:

```
isolation.tools.copy.enable=false
isolation.tools.paste.enable=false
isolation.tools.setGUIOptions.enable=false
```

Required set-uid programs:

```
pam_timestamp_check, passwd, pwdb_chkpwd, su, unix_chkpwd, vmkload_app, vmware-authd,
vmware-vmx
```

Optional:

```
crontab, ping, sudo, vmkping
```

Special case:

```
ssh-keysign
```

Make sure there is at least one user in the wheel group, then uncomment:

```
"auth required /lib/security/$ISA/pam_wheel.so
use_uid" in /etc/pam.d/su
```

Additionally, HyTrust establishes a system for rotating root passwords for the VMware ESX servers under HyTrust protection and allowing authorized users to check out one-time use time-limited auto-generated root passwords.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  HyTrust Appliance is a closed system based on the CentOS operating system, which implements a limited number of necessary services. Additional security features include the following:

  - Production services run unprivileged
  - No root login is allowed
  - The HTA administrator account is unprivileged
  - Sudoers-based privilege escalation
  - All unencrypted services disabled by default

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for* *example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

HyTrust Appliance has the capability to download security updates and fixes directly from the HyTrust web site. When this is enabled, updates are downloaded and installed automatically. Updates can also be distributed as ISO packages and installed manually. To prevent Trojan attacks, HyTrust updates and HTA licenses are signed and validated using public keys.

Updates provided via this facility include security updates to the CentOS, application stack, and software developed by HyTrust.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

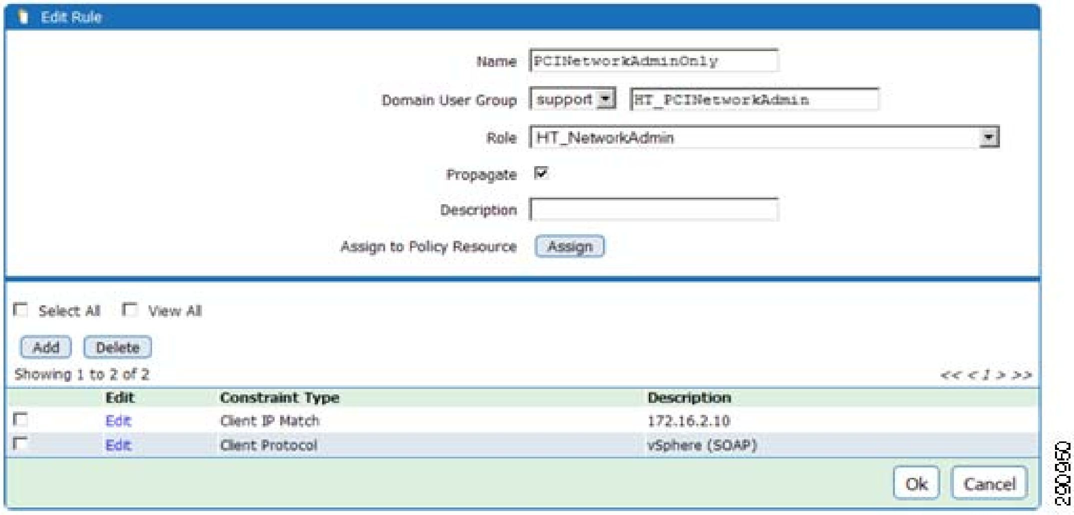
The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory, which is linked via LDAP, RADIUS, and TACACS+ services). Individual user IDs are assigned. Roles are defined and based on group membership. HyTrust Appliance connects to this resource via LDAP to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

HyTrust Appliance implements a sophisticated policy-driven access control system that makes an authorization decision for every attempted operation in the Vblock environment. The authorization decision is based on the user ID as obtained from the vSphere session, the user function as derived from the user's assigned role in Active Directory, logical infrastructure segmentation, least privilege role defined for this activity, and object-level policy active for that user.

In the reference implementation, a policy was created that restricted CDE virtual systems to operating only on the PCI portion of the infrastructure and enforced separation of duties between the network administrators and CDE application owners.

Figure 5-86 Edit Rule Screen



Edit Rule

Name: PCINetworkAdminOnly

Domain User Group: support ▾ HT_PCINetworkAdmin

Role: HT_NetworkAdmin ▾

Propagate: ☑

Description:

Assign to Policy Resource: Assign

□ Select All □ View All

Add Delete

Showing 1 to 2 of 2 << < 1 > >>

	Edit	Constraint Type	Description
□	Edit	Client IP Match	172.16.2.10
□	Edit	Client Protocol	vSphere (SOAP)

Policy and privilege definition was performed by a separate group of authorized users, typically security professionals.

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  HyTrust Appliance implements default "deny all" access policy. Many of the users that gain access to Vblock infrastructure by the means of HyTrust Appliance proxying their operations do not have privileges to log into the HyTrust Appliance management console.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing LDAP to the domain controller for AAA services and Microsoft Active Directory policy for user account services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

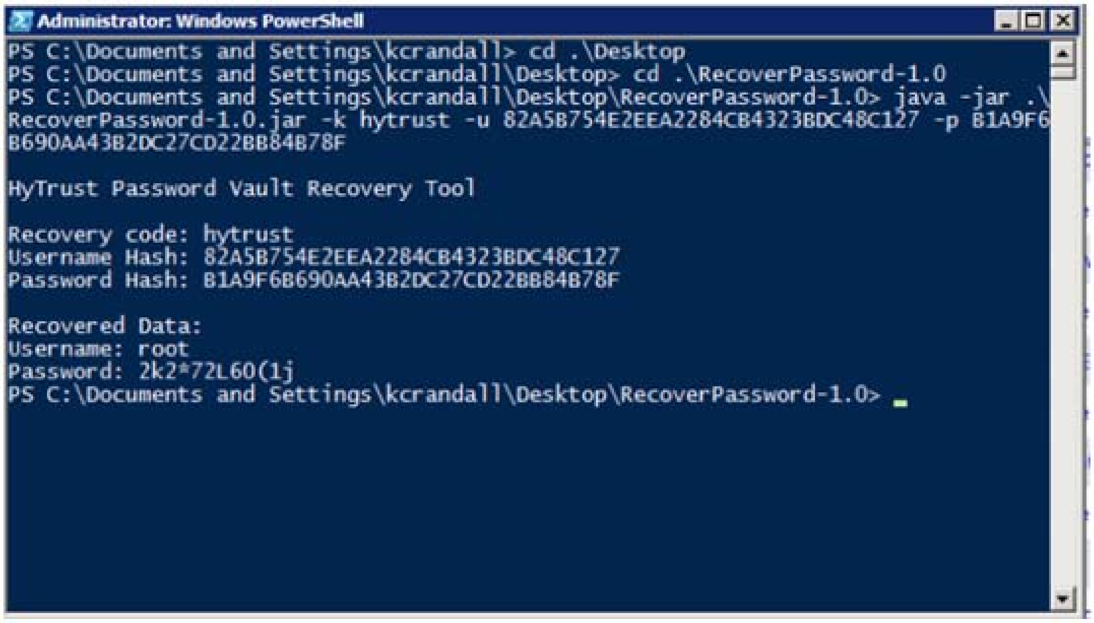
  Sub-requirement 8.2 is met by supporting RSA two-factor authentication where the user enters the AD password (something they know) in conjunction with an RSA physical token (something they have).

  HyTrust Appliance acts as a compensating control for the Vblock infrastructure and enables RSA two-factor authentication to work with any methods of access to VMware vSphere or Cisco Nexus 1000V.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.8**—
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  HyTrust Appliance enforces the use of one-time root passwords for all VMware ESX hosts in the environment. Unique random machine-generated passwords of 12 characters in length are set up for each host and rotated every five days (see Figure 5-87). If requested by a privileged user, a different one-time use password was generated and remained valid for a fixed time duration not to exceed 24 hours. Sub-requirement 8.5.8 was met by allowing only one temporary use password to be issued at the time, thus associating the password with a specific user who was issued the password.

Figure 5-87 Using Root Passwords



```
PS C:\Documents and Settings\kcrandall> cd .\Desktop
PS C:\Documents and Settings\kcrandall\Desktop> cd .\RecoverPassword-1.0
PS C:\Documents and Settings\kcrandall\Desktop\RecoverPassword-1.0> java -jar .\
RecoverPassword-1.0.jar -k hytrust -u 82A5B754E2EEA2284CB4323BDC48C127 -p B1A9F6
B690AA43B2DC27CD22BB84B78F

HyTrust Password Vault Recovery Tool

Recovery code: hytrust
Username Hash: 82A5B754E2EEA2284CB4323BDC48C127
Password Hash: B1A9F6B690AA43B2DC27CD22BB84B78F

Recovered Data:
Username: root
Password: 2k2*72L60(1j
PS C:\Documents and Settings\kcrandall\Desktop\RecoverPassword-1.0> _
```

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Sub-requirements 8.1, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, and 8.5.15 were met by integrating HyTrust Appliance authentication with Microsoft Active Directory. User accounts and passwords are not managed on HyTrust Appliance; instead, when authentication is requested by the user, HyTrust Appliance performs the actual authentication request against Active Directory. Complex AD environments with multiple domains are supported for authentication.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

HyTrust Appliance is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*

- **PCI 10.2.5**—*Use of identification and authentication mechanisms*
- **PCI 10.2.6**—*Initialization of the audit logs*
- **PCI 10.2.7**—*Creation and deletion of system-level objects*

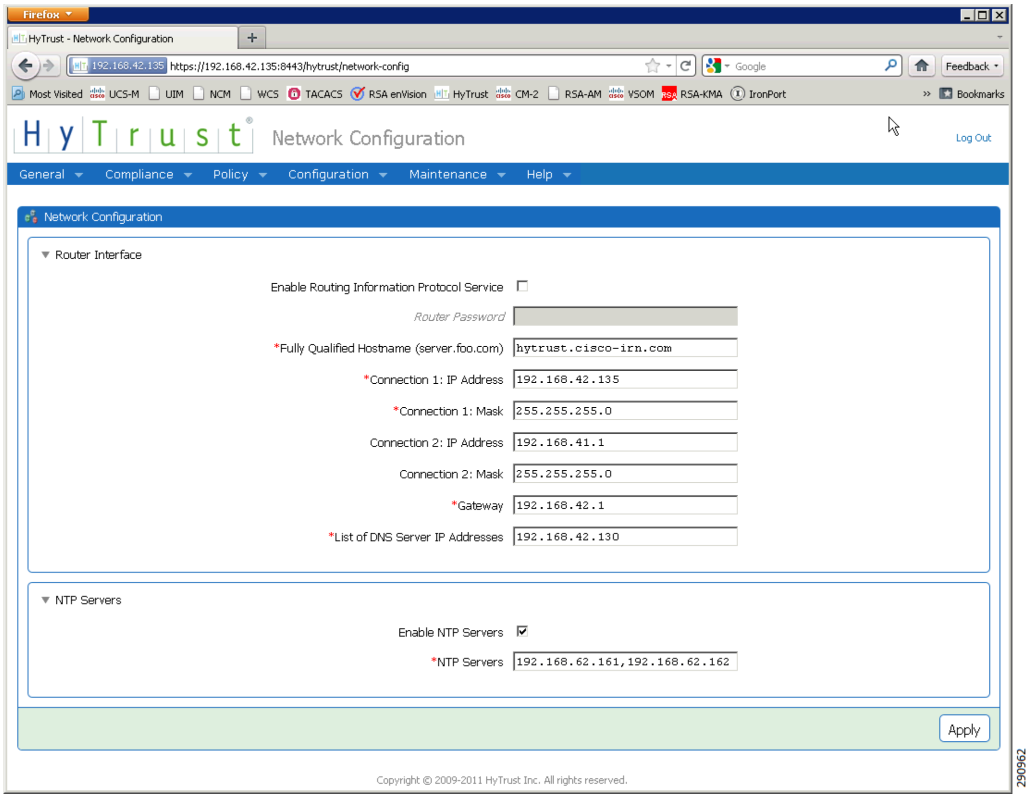
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

HyTrust Appliance uses NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. The HyTrust Appliance uses NTP to meet these requirements by specifying the NTP server in the IP settings. (See Figure 5-88.)

Figure 5-88 Specifying the NTP Server



Enable Routing Information Protocol Service □

Router Password

*Fully Qualified Hostname (server.foo.com) hytrust.cisco-irn.com

*Connection 1: IP Address 192.168.42.135

*Connection 1: Mask 255.255.255.0

Connection 2: IP Address 192.168.41.1

Connection 2: Mask 255.255.255.0

*Gateway 192.168.42.1

*List of DNS Server IP Addresses 192.168.42.130

Enable NTP Servers ☑

*NTP Servers 192.168.62.161,192.168.62.162

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Additional In Scope Devices

Any system that stores, processes, or transmits cardholder data is considered in scope for PCI compliance. Infrastructure components that provide network services such as load balancing or WAN optimization are often not considered when contemplating compliance. However, if these technologies pass sensitive data, they are subject to the same controls of traditional security products.

The capabilities that these components need to meet are highlighted in Table 5-1.

Infrastructure

Routing

Router—Store

The Cisco Integrated Services Router (ISR) is the component that is used as the primary routing and security platform of the stores. It can securely scale to the requirements of the business because it has integrated firewall, VPN, and IPS/IDS capabilities. WAN options include traditional terrestrial paths using T1, T3, Ethernet, and so on; wireless options include 3G/4G/Wi-Fi modules connecting stores over public paths for higher availability.

The Cisco ISR consolidates voice, data, and security into a single platform with local and centralized management services. It delivers scalable rich media, service virtualization, and energy efficiency ideal for deployments requiring business continuity, WAN flexibility, and superior collaboration capabilities. The Cisco ISR uses field-upgradeable motherboards, with services such as security, mobility, WAN optimization, unified communications, video, and customized applications.

Table 5-36 lists the performance of the Cisco ISR in satisfying PCI sub-requirements.

Table 5-36 PCI Assessment Summary—Cisco ISR

Models Assessed	
CISCO891W version c890-universalk9-mz.151-3.T.bin CISCO1941W-A/K9 version c1900-universalk9-mz.SPA.151-3.T.bin CISCO2921/K9 version c2900-universalk9-mz.SPA.151-3.T.bin CISCO2951/K9 version c2951-universalk9-mz.SPA.151-3.T.bin CISCO3945-SPE150/K9 version c3900-universalk9-mz.SPA.151-3.T.bin	
PCI Sub-Requirements Passed	
PCI 1	1.2.1, 1.2.2, 1.2.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 4	4.1
PCI 6	6.1
PCI 7	7.7.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10. 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1,10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI 11	11.4
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of the Cisco ISR is the segmentation of PCI scope and enforcement of that new scope boundary.

It has five primary functions/capabilities in relation to PCI.

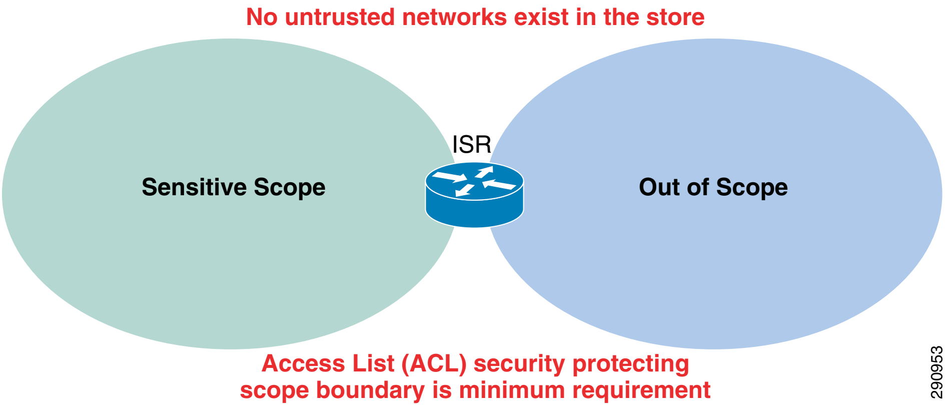
1. As a router, directing traffic between networks

   A router in its simplest form routes between networks. By segmenting a network into sub-networks, a retailer can isolate sensitive information from non-sensitive information. The Cisco ISR can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's cardholder data environment. Depending on risk vectors within the store, different levels of enforcement might be required at the segmented scope boundary level. (See items 2, 3 and 4 following.)

2. As a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network

   A router with ACLs can be used to enforce segmented traffic only if the ACLs are used to filter and segment private networks of the retailer. They may not be used to filter untrusted networks. For example, many retailers have a central chokepoint in their data center that is the connection to the Internet (an untrusted network). As long as the retailer has only untrusted network connections outside of the store, (the data center, in this case), then a retailer may use router access lists to protect its scope from its own private internal networks. As soon as the store connects to untrusted networks directly, items 3 and 4 below become relevant. (See Figure 5-89.)

Figure 5-89 ACLs Segment Traffic


No untrusted networks exist in the store
ISR
Sensitive Scope
Out of Scope
Access List (ACL) security protecting
scope boundary is minimum requirement
290953

3. As a stateful firewall, restricting traffic between the cardholder data environment and other areas of the network

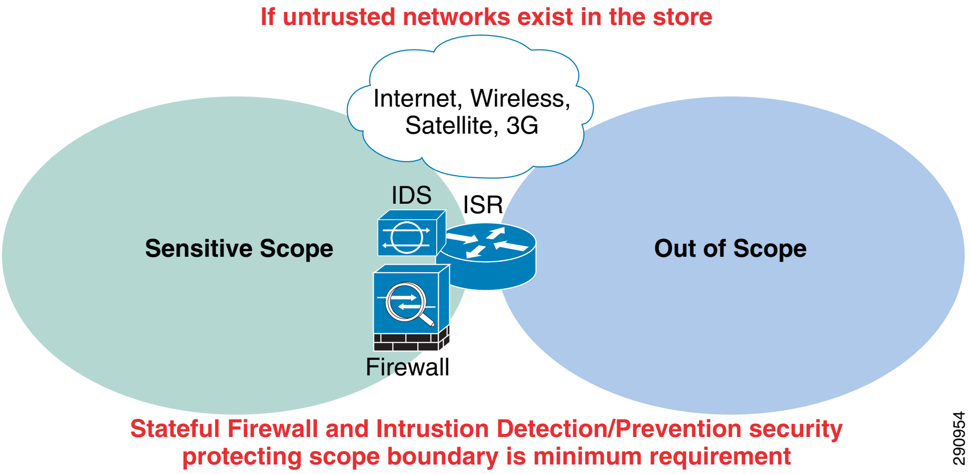
   As soon as any untrusted network is introduced at the store level, firewalling and IDS/IPS must be deployed. The following are examples of untrusted networks:

   - The Internet
   - Wireless
   - Satellite
   - 3G/4G cellular backup

4. As an intrusion prevention system, inspecting all traffic going to and from the cardholder data environment

   As soon as any untrusted network is introduced at the store level, firewalling and IDS/IPS must be deployed. (See Figure 5-90.)

Figure 5-90 Using Firewall and IDS/IPS


If untrusted networks exist in the store
Internet, Wireless,
Satellite, 3G
IDS
ISR
Sensitive Scope
Out of Scope
Firewall
Stateful Firewall and Intrustion Detection/Prevention security
protecting scope boundary is minimum requirement
290954

The Cisco ISR can be used to address segmentation challenges and enforce scope boundaries depending on the levels required by the retailer. Each of these features can be enabled by using a license key. This feature is particularly useful for retailers because it does not require a visit to every store to enable the firewall/IPS/IDS capability. If these capabilities are not used within the Cisco ISR, an external component(s) can be used to address this level of scope enforcement.

5. As a VPN system, encrypting all traffic going to and from the store across open and public networks.

   The Cisco ISR can be used to address the need to encrypt the transmission of cardholder data across open, public networks such as 3G/4G/Wi-fi, and satellite technologies using SSL and IPSec technologies.

Table 5-36 lists the component assessment details for the Cisco ISR.

Table 5-37 Component Capability Assessment—Cisco ISR

Cisco ISR	
PRIMARY FUNCTION	**Requirement 1, 11 (1.2, 1.3, 11.4)**
Protect trusted networks from untrusted networks with ACLs or firewall/IDS/IPS.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- The security features of the Cisco ISR routers in the store designs are configured using Cisco Security Manager. When adopting this as the primary method of router configuration, Cisco does not recommend making changes directly to the command-line interface (CLI) of the router. Unpredictable results can occur when central and local management are used concurrently.
- The general configuration of the Cisco ISR routers in the store architectures are maintained with EMC Ionix Network Configuration Manager.

- Firewall rule sets must adhere to a “least amount of access necessary” policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment (for example, point-of-sale) networks.
- Ensure that inspection rules and/or zones are enabled on the Cisco ISR router so that the firewall maintains state (none are enabled by default).
- Redundant Cisco IOS firewalls do not have the capability to maintain state between the routers. During a failure, client communication sessions need to be re-established through the alternate router. If high availability with statefulness is a requirement, Cisco ASA firewalls should be used.
- Access into a store router from the WAN needs to be protected by a store-located firewall filter if the WAN technology is considered untrusted/public (for example, Internet DSL or cable network, public 3G or 4G, satellite). In the Cisco Retail PCI Solution lab, a private MPLS WAN is simulated, and filtering of the store traffic occurs on the WAN link of all in-scope locations.
- Disable the HTTP server service on the router and enable the HTTP secure server.
- Disable use of Telnet and enable use of only SSH version 2.
- Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, VTY, and line interfaces on the router. Disable the AUX interface.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the router.
- Change default passwords and community strings to appropriate complexity.
- Configure logs to be sent to a centralized syslog server, such as RSA enVision.
- Configure NTP to ensure all logging is coordinated.
- Disable un-necessary services (for example, Bootp, Pad, ipv6).
- Shutdown unused interfaces.

Each of the store designs was implemented using guidance from the following:

- Cisco Enterprise Branch Security Design Guide—
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/E_B_SDC1.html
- Branch/WAN Design Zone—
  http://www.cisco.com/en/US/netsol/ns816/networking_solutions_design_guidances_list.html

Additional information for router hardening can be found at the following URLs:

- Cisco Guide to Harden Cisco IOS Devices—
  http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
- Cisco IOS Security Configuration Guide, Release 12.4—
  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco zone-based firewalls are configurable to restrict traffic through the use of class map, policy map, and zone pair service policy statements and access lists.

- **PCI 1.2.2**—*Secure and synchronize router configuration files*

  Router configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of routers and switches are synchronized.

- **PCI 1.2.3**—*Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.*

  Cisco zone-based firewalls are configured with source and destination zones to control traffic passing from one zone to another. Each of these zone pairs receives a service policy, which is the mechanism that identifies permitted traffic, while all other traffic is dropped and logged.

  ```
  zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
   service-policy type inspect CSM_ZBF_POLICY_MAP_18
  ```

- **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*

  Router WAN interfaces connected to public network connections such as the Internet should have filtering applied to prevent spoofing of both public and private IP address. Typical filters for private IP address blocks are as follows:

  ```
  ip access-list extended COARSE-FILTER-INTERNET-IN
   remark -------------------------------------------------------
   remark ---Block Private Networks---
   deny   ip 10.0.0.0 0.255.255.255 any log
   deny   ip 172.16.0.0 0.15.255.255 any log
   deny   ip 192.168.0.0 0.0.255.255 any log
   remark -
   remark ---Block Autoconfiguration Networks---
   deny   ip 169.254.0.0 0.0.255.255 any log
   remark -
   remark ---Block Loopback Networks---
   deny   ip 127.0.0.0 0.0.255.255 any log
   remark -
   remark ---Block Multicast Networks---
   deny   ip 224.0.0.0 15.255.255.255 any log
   remark -
   remark ---Block Your assigned IP’s at edge---
   deny   ip <YOUR_CIDR_BLOCK> any log
   remark -
   remark ---Allow remaining public internet traffic---
   permit ip any any
  ```

- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*

  Cisco zone-based firewalls are configured with source and destination zones to control traffic passing from one zone to another. Each of these zone pairs receives a service policy, which is the mechanism that identifies permitted traffic, while all other traffic is dropped and logged.

  ```
  zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
   service-policy type inspect CSM_ZBF_POLICY_MAP_16
  ```

- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*

  Cisco zone-based firewalls are configurable to perform stateful inspection by use of the *inspect* statement in the associated class map, policy map, and zone pair service policy statements.

  ```
  class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
   match access-group name CSM_ZBF_CMAP_ACL_9
   match protocol tcp

  policy-map type inspect CSM_ZBF_POLICY_MAP_7
   class type inspect CSM_ZBF_CLASS_MAP_9
    inspect Inspect-1
   class type inspect CSM_ZBF_CLASS_MAP_10
    inspect Inspect-1
   class type inspect CSM_ZBF_CLASS_MAP_11
    inspect Inspect-1
   class class-default
    drop log

  zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
   service-policy type inspect CSM_ZBF_POLICY_MAP_7
  ```

- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*

  In the store design, VLANs are used to segment traffic based on function and security requirements. Each of these VLANs are assigned to an appropriate security zone using the zone-based firewall feature of the router.

  ```
  interface GigabitEthernet0/0.11
   description POS
   zone-member security S_POS
  interface GigabitEthernet0/0.13
   description VOICE
   zone-member security S_Voice
  ```

- **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco routers can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management, IPsec VPN for remote connectivity, and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists.

```
no ip http server
ip http secure-server
snmp-server user remoteuser remoteuser v3
line vty 0 4
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 transport preferred none
 transport input ssh
 transport output none
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco routers have several services that are enabled by default that need to be disabled:

```
no service pad
no service udp-small-servers
no service tcp-small-servers
no ip bootp server
no mop enable
no service finger
no ip forward-protocol nd
no ip http server
```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco routers support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

Note Strong cryptography—Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Before Crypto keys can be generated hostname and domain name must be entered

hostname R-A2-Small-1
ip domain name cisco-irn.com

! Generate keys with 1024 or larger bit key generation NOT the default 512

Crypto key generate rsa

ip ssh version 2

ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

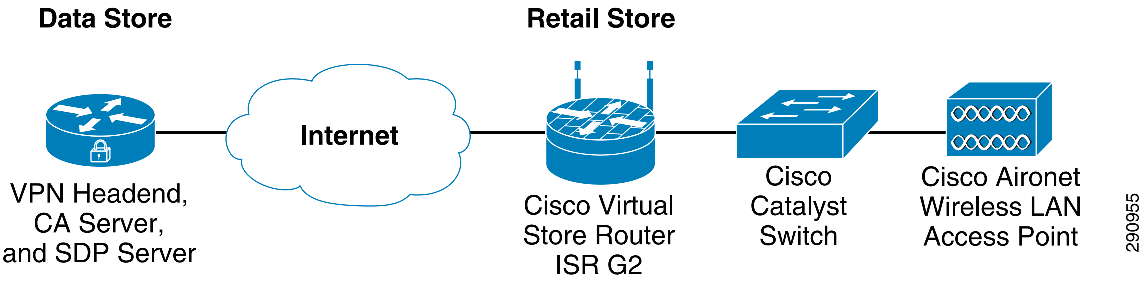
- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

  Public WAN link connections include technologies such as DSL, cable, satellite, Wi-Fi, and 3G/4G networks. These are considered untrusted public networks within PCI. A VPN is required to securely tunnel traffic between the store and the enterprise network.

  Cisco Virtual Office provides reference designs for building a VPN solution to connect stores to data centers using these technologies. For more information about Cisco VPN solutions, see: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6808/prod_white_paper0900aecd8051bf3b_ns855_Networking_Solutions_White_Paper.html

  The following example describes equipment located at the store and the data center headend router. The store router is referred to as the spoke router, and the data center router as the hub. Figure 5-91 shows a simplified Cisco VPN topology.

Figure 5-91 Cisco VPN Topology



Cisco VPN technology connects the stores to the data center over the Internet. As a result, a secure, encrypted tunnel is used to secure sensitive information such as cardholder data. Cisco VPN technologies offer a choice to protect the data in transit and provide a secure access to the stores' networks, including Easy VPN and Dynamic Multipoint VPN (DMVPN).

This example shows DMVPN as the VPN technology. DMVPN uses IPSec-encrypted GRE tunnels, with dynamic routing. Two simultaneously active DMVPN tunnels are built from each store to different hub routers, providing instant failover. If the primary tunnel fails, routing converges to use the secondary tunnel, and all sessions are kept alive. In addition, with DMVPN, store routers can dynamically build spoke-to-spoke tunnels between each other to exchange data, without having to tunnel the traffic back to the hub, thus alleviating the load on the headend.

Following are sample DMVPN spoke and hub configurations. Enhanced Interior Gateway Routing Protocol (EIGRP) is used as the routing protocol inside the DMVPN network. Split-tunneling is used and only traffic on the POS and employee VLANs going to the servers on the 10.0.0.0 network at the headquarters is sent through the DMVPN tunnel, while any other traffic is sent straight to the Internet. Note that, if split-tunneling is not required, a default route (to 0.0.0.0) can be advertised from the hubs to the spokes, instead of specific subnets.

891 Store Router

```
!! Configure the IP addresses on the VLAN interfaces
interface vlan 10
  description POS VLAN
  ip address 172.16.10.1 255.255.255.0
  no autostate
interface vlan 20
  description employee VLAN
  ip address 172.16.20.1 255.255.255.0
  no autostate
interface vlan 30
  description guest VLAN
  ip address 172.16.30.1 255.255.255.0
  no autostate
!! Configure the ISAKMP and IPSec policies
crypto isakmp policy 1
  encryption aes 256

crypto isakmp keepalive 35 5
crypto isakmp nat keepalive 10
crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
 mode transport

crypto ipsec profile cvs
 set transform-set t1
ip multicast-routing
!! Configure the DMVPN tunnel
interface Tunnel0
  bandwidth 1000
  ip address 192.168.1.3 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip hello-interval eigrp 99 30
  ip hold-time eigrp 99 90
  ip pim sparse-dense-mode
  ip nhrp map multicast <Primary-hub-public-IP>
  ip nhrp map 192.168.1.1 <Primary-hub-public-IP>
  ip nhrp nhs 192.168.1.1
  ip nhrp map multicast <Secondary-hub-public-IP>
  ip nhrp map 192.168.1.2 <Secondary-hub-public-IP>
  ip nhrp nhs 192.168.1.2
  ip nhrp authentication <password>
  ip nhrp network-id 12345
  ip nhrp holdtime 300
  ip nhrp registration no-unique
  ip nhrp shortcut
  ip nhrp redirect
  ip tcp adjust-mss 1360
  load-interval 30
  delay 1000
  qos pre-classify
  tunnel source GigabitEthernet0
  tunnel mode gre multipoint
  tunnel key 12345
  tunnel protection ipsec profile cvs


!! Configure the DMVPN routing protocol. Only permit the POS and employee LAN !!
subnets to be advertised to the hubs
ip access-list standard dmvpn_acl
  permit 172.16.10.0 0.0.0.255
  permit 172.16.20.0 0.0.0.255
```

```
router eigrp 99
  no auto-summary
  network 192.168.1.3 0.0.0.0
  network 172.16.10.1 0.0.0.0
  network 172.16.20.1 0.0.0.0
  distribute-list dmvpn_acl out
```

3945E Hub Router:

```
!! Configure the ISAKMP and IPSec policies

crypto isakmp policy 1
  encryption aes 256

crypto isakmp keepalive 35 5
crypto isakmp nat keepalive 10

crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
  mode transport require

crypto ipsec profile cvs
  set transform-set t1

!! Enable multicast routing

ip multicast-routing

!! Configure the DMVPN tunnel. Use the same bandwidth metric for both primary !! and
secondary hubs, but a lower delay metric on the primary hub

interface Tunnel0

  bandwidth 2000
  ip address 192.168.1.1 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip pim sparse-dense-mode
  ip nhrp authentication <password>
  ip nhrp map multicast dynamic
  ip nhrp network-id 12345
  ip nhrp redirect
  ip tcp adjust-mss 1360
  no ip split-horizon eigrp 99
  delay 1000
  qos pre-classify
  tunnel source <Outside_Interface >
  tunnel mode gre multipoint
  tunnel key 12345
  tunnel protection ipsec profile cvs

!! Configure the DMVPN routing protocol. Only the 10.0.0.0 network is        !!
advertised to the spokes in this example (split-tunneling)

router eigrp 99
  no auto-summary
  network 192.168.1.1 0.0.0.0
  redistribute static route-map split_in
ip access-list standard split_in
  permit 10.0.0.0

route-map split_in permit 10
  match ip address split_in
```

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Integrated Services Routers. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco routers are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco routers, no users are allowed access unless specifically configured and assigned appropriate passwords.

```
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration, as specified in PCI requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

These AAA authentication groups are assigned to the administrative interfaces where users connect:

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

Services provide on-going access to software updates and security patches for a variety of Cisco products.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

The router is able to meet some of the requirements locally, as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco routers support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco routers require setting of a password.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the routers also support the use of AES encryption of pre-shared keys.

```
service password-encryption
password encryption aes
```

Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fall back user accounts.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco routers do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco routers do not support an automated capability to perform this function at this time, user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco routers support the ability to specify a minimum password length for local accounts.

  ```
  security passwords min-length 7
  ```

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco routers do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco routers do not support an automated capability to perform this function at this time: user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco routers support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco routers support the local ability to block logins after a specified time after failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco router management interfaces are configured as follows to meet this requirement:

  ```
  ip http timeout-policy idle 900

  line con 0
  ```

```
 session-timeout 15 output
 exec-timeout 15 0
line vty 0 4
 session-timeout 15  output
 exec-timeout 15 0
line vty 5 15
 session-timeout 15  output
 exec-timeout 15 0
```

Note If only the **session timeout** command is specified, the session timeout interval is based solely on detected input from the user. If the **session timeout** command is specified with the **output** keyword, the interval is based on both input and output traffic. You can specify a session timeout on each port. The **session-timeout** command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state. You can use a combination of the **exec-timeout** and **session-timeout** line configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the **session-timeout** command causes on physical lines.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco ISRs are able to track and monitor all administrative user access and events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco routers track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

The Cisco ISR uses Network Time Protocol (NTP) to update and synchronize their local clock facilities and meet sub-requirements 10.4.1 through 10.4.3:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco routers use NTP to meet these requirements by implementing the following configuration statements:

  ```
  ntp server 192.168.62.161 prefer
  ntp server 192.168.62.162

  clock timezone PST -8 0
  clock summer-time PDT recurring

  service timestamps debug datetime localtime show-timezone
  service timestamps log datetime msec localtime show-timezone
  ```

  To learn more about NTP, visit the following URL:
  http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Requirement 10.5 was met using RSA enVision, a central logging repository that collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.4**—*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.*

Cisco routers are capable of performing intrusion detection. Each of the store reference designs includes untrusted networks (either a public Internet connection or wireless networks); therefore, intrusion detection capabilities are required. IPS signature updates and configurations are managed centrally through Cisco Security Manager, which implements the following configuration statements to enable the IPS inspection capability in the routers:

```
ip ips config location flash0: retries 1 timeout 1
ip ips notify SDEE
ip ips name Store-IPS
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
interface GigabitEthernet0/0
 description WAN
 ip ips Store-IPS in
 ip ips Store-IPS out
interface GigabitEthernet0/1.11
 description POS
 ip ips Store-IPS in
 ip ips Store-IPS out
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 ip ips Store-IPS in
 ip ips Store-IPS out
```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Routers—Data Center

The primary function of data center routers from a PCI perspective is routing between sensitive networks and out-of scope networks. Data center routers function as WAN aggregation routers or connecting to larger networks such as the Internet. Therefore, performance and scalability are equally important as securely passing data. For this reason, and unlike the routers in the store, security functions are typically separated physically into distinct appliances. The Cisco 7206VXR and the the Cisco ASR1002 routers were used for the Internet edge and store WAN edge portions of the network within the solution testing.

Primary PCI Function

The main function of the data center routers is the segmentation of PCI scope and enforcement of that new scope boundary. The data center router has four primary functions/capabilities in relation to PCI:

1. As a router, directing traffic between networks

   A router in its simplest form routes between networks. By segmenting a network into sub-networks, a retailer can isolate sensitive information from non-sensitive information. Data center routers can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's cardholder data environment. Depending on risk vectors, different levels of enforcement might be required at the segmented scope boundary level. (See items 2, 3, and 4 following.)

2. As a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network

   A router with ACLs can be used to enforce segmented traffic only if the ACLs are used to filter and segment private networks of the retailer. They may not be used to filter untrusted networks. For example, if a data center router is used to segment sensitive PCI networks from internal inventory networks, a retailer may use router access lists to protect its scope. As soon as the store connects to untrusted networks directly, items 3 and 4 below become relevant.

3. As a stateful firewall, restricting traffic between the cardholder data environment and other areas of the network

   As soon as any untrusted network is introduced to the connections of the data center router, firewalling and IDS/IPS must be deployed. The following are examples of untrusted networks:

   - Internet
   - Wireless
   - Satellite
   - Cellular backup

4. As an intrusion prevention system, inspecting all traffic going to and from the cardholder data environment

   As soon as any untrusted network is introduced to the connections of the data center router, firewalling and IDS/IPS must be deployed at that location.

Table 5-38 PCI Assessment Summary—Data Center Routers

Models Assessed	
CISCO7206VXR-NPE-G1 version c7200-advipservicesk9-mz.124-24.T4.bin, ASR-1002 (RP1) version asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin	
PCI Sub-Requirements Passed	
PCI 1	1.2.2, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8
PCI 2	2.2, 2.2.2, 2.2.3, 2.2.4, 2.3
PCI 4	4.1
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The data center routers protect trusted networks from untrusted networks with ACLs or firewall/IDS/IOS. (1.2, 1.3, 11.4)

Table 5-38 lists the component assessment details for the Cisco data center routers.

Table 5-39 Component Capability Assessment—Data Center Routers

Data Center Routers	
PRIMARY FUNCTION	Requirement 1, 11 (1.2, 1.3, 11.4)
Protect trusted networks from untrusted networks with ACLs or firewall/IDS IOS.	
CAPABILITY	ASSESSMENT
Secure Services	
Disabled any unnecessary services—*“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- Configuration was done manually on the router CLI, and backup of configuration and monitoring of configuration for changes and non-compliance were done through the EMC Ionix Network Configuration Manager (alternatively, CiscoWorks Resource Manager Essentials, a component of Cisco LMS, can be used as well).
- The perimeter firewalling of the data center was provided by the Cisco ASA. As a result, the Cisco 7206VXR and the Cisco ASR1002 were not evaluated according to the set of 1.x requirements for firewalls.
- Disable the HTTP server service on the router and enable the HTTP secure server.
- Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, VTY, and line interfaces on the router. Disable the AUX interface.

- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the router.
- Enable anti-spoofing on all interfaces.
- Routers in the data center were implemented using guidance from the following:
  - Enterprise Data Center Design guide based on a Data Center 3.0 Architecture— http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html
  - Enterprise Internet Edge Design Guide— http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html
- For the Internet edge routers, use the access list below on the interface that is facing the Internet. This access list explicitly filters traffic destined for the infrastructure address space. Deployment of edge infrastructure access lists requires that you clearly define your infrastructure space and the required/authorized protocols that access this space. The access list is applied at the ingress to your network on all externally facing connections, such as peering connections, customer connections, and so forth.

```
!
ip access-list extended COARSE-FILTER-INTERNET-IN
 remark -------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Your assigned IP's at edge---
 deny   ip <YOUR_CIDR_BLOCK> any log
 remark -
 remark ---Allow remaining public internet traffic---
 permit ip any any
!
```

Note The **log** keyword can be used to provide additional details about source and destinations for a given protocol. Although this keyword provides valuable insight into the details of access list hits, excessive hits to an access list entry that uses the **log** keyword increase CPU utilization. The performance impact associated with logging varies by platform.

The service provider network in the solution represented an Multiprotocol Label Switching (MPLS) network. At the writing of this document, MPLS is considered a private network, and secure tunneling across the WAN is not required. MPLS implementations may be public or private with regards to PCI,

depending on how the service provider implements the MPLS network and whether the provider has satisfactorily completed their annual PCI audit. For best practices when in doubt, Cisco recommends VPN tunneling be implemented. For further information on implementing an IPSec VPN, see the *IPSec VPN Direct Encapsulation Design Guide* at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Dir_Encap.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Router configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of routers and switches are synchronized.

- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*

  PCI 1.3.8—*Do not disclose private IP addresses and routing information to unauthorized parties.*

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco routers can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management, IPsec VPN for remote connectivity, and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists:

```
no ip http server
ip http secure-server
ip scp server enable
snmp-server user remoteuser remoteuser v3
line vty 0 4
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 transport preferred none
 transport input ssh
 transport output none
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco routers have several services that are enabled by default that can be disabled:

  ```
  no service pad
  no service udp-small-servers
  no service tcp-small-servers
  no ip bootp server
  no mop enable
  no service finger
  no ip forward-protocol nd
  no ip http server
  ```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco routers support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

Note Strong cryptography is based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Before Crypto keys can be generated hostname and domain name must be entered

hostname RWAN-1
ip domain name cisco-irn.com

! Generate keys with 1024 or larger bit key generation NOT the default 512

Crypto key generate rsa

ip ssh version 2

ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco routers. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco routers are configured to use a AAA model for user-based access. Users can be assigned to groups, and based on privilege levels, have access to only the information they require for their job function. By default in Cisco routers, no users are allowed access unless specifically configured and assigned appropriate passwords.

```
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

The following AAA authentication groups are assigned to the administrative interfaces where users connect:

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco routers to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure ACS must be implemented. Configure AAA services as shown above in Requirement 7.

The router is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco routers support the creation of local user accounts with unique ID's through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco routers require the setting of a password.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the routers also support the use of AES encryption of pre-shared keys.

  ```
  service password-encryption
  ```

```
password encryption aes
```

Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fallback user accounts.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco routers do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco routers do not support an automated capability to perform this function at this time, user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco routers support the ability to specify a minimum password length for local accounts.

  ```
  security passwords min-length 7
  ```

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco routers do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco routers do not support an automated capability to perform this function at this time: user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco routers support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco routers support the local ability to block logins after a specified time after failed login attempts with the following command:

```
login block-for 1800 attempts 6 within 65535
```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco router management interfaces are configured as follows to meet this requirement:

```
ip http timeout-policy idle 900

line con 0
 session-timeout 15 output
```

```
 exec-timeout 15 0
line vty 0 4
 session-timeout 15  output
 exec-timeout 15 0
line vty 5 15
 session-timeout 15  output
 exec-timeout 15 0
```

Note If only the **session timeout** command is specified, the session timeout interval is based solely on detected input from the user.

If the **session timeout** command is specified with the **output** keyword, the interval is based on both input and output traffic.You can specify a session timeout on each port.

The **session-timeout** command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state.

You can use a combination of the **exec-timeout** and **session-timeout** line configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the **session-timeout** command causes on physical lines.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco routers are able to track and monitor all administrative user access and events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco routers track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

Cisco routers use NTP to update and synchronize their local clock facilities and meet sub-requirements 10.4 through 10.4.3.

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco routers use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Note The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Switching

Switches—Store

Cisco store switches provide connectivity for wired endpoints and the ability to segment them onto their own sensitive scope networks. Virtual local area networks (VLANs) are used to put sensitive PCI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks.

Store switches are broken into three categories to provide scale and feature relevance;

- Compact switches—Quiet, small form factor switches that can be used on store floors to extend the capability of the network to the register. These switches use power over Ethernet (PoE) pass-through, reducing expensive power and network cabling costs to new devices at the area of sale.
- Access switches—Stackable, expandable switches that can be used for wired device port density in the store wiring closets. Access switches offer a variety of modular and fixed configuration options, and feature operational efficiency with StackPower, FlexStack, and NetFlow to increase visibility and control.
- Core/distribution—Highly redundant, powerful core switches allow for the most demanding business requirements of the store. Modular functionality provides the ability to insert security technology as the needs of the business expand into new areas.

Table 5-40 PCI Assessment Summary—Store Switches

Models Assessed	
WS-C3560E-PS-24c3560e-universalk9-mz.122-35.SE5.bin WS-C2960PD-8TT-Lc2960-lanbasek9-mz.122-55.SE1.bin WS-C2960G-8TC-Lc2960-lanbasek9-mz.122-50.SE4.bin WS-C2960-8TC-Lc2960-lanbasek9-mz.122-50.SE4.bin WS-C2960S-48FPS-Lc2960s-universalk9-mz.122-53.SE1.bin WS-C3750X-48PF-Sc3750e-universalk9-mz.122-53.SE2.bin WS-C2960CPD-8PT-Lc2960c405-universalk9-mz.122-55.0.43.SK.bin WS-4507+R SUP-7cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin WS-C3560X-48PF-Sc3560e-universalk9-mz.122-53.SE2.bin WS-C3560CPD-8PT-Lc3560c405ex-universalk9-mz.122-55.0.44.SK.bin	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15

Table 5-40 PCI Assessment Summary—Store Switches (continued)

PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI 11	11.1.b, 11.1.d
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

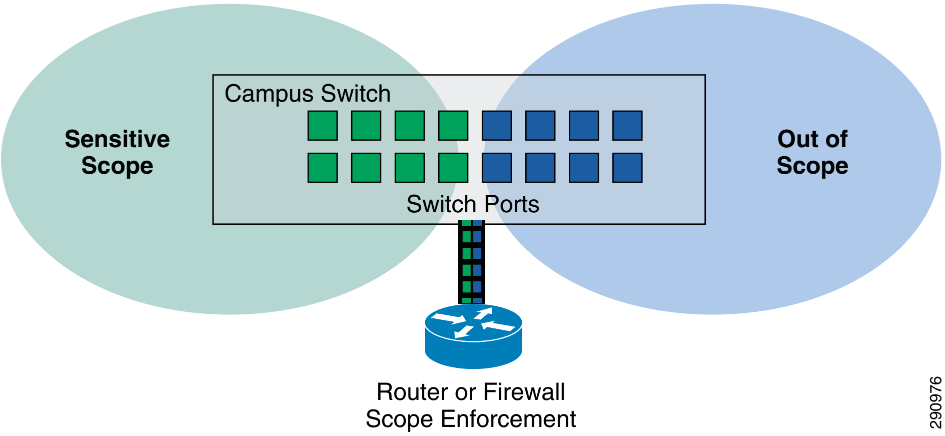
Primary PCI Function

The primary PCI compliance feature of store switches is to provide secure wired port access. (9.1.2, 11.1)

Store switches also provide PCI compliance via segmentation of sensitive networks from out-of-scope networks. Although technically a firewall or ACL is used to enforce PCI Requirement 1, switches extend that Layer 3 boundary to Layer 2. Using VLANs, Cisco store switches allow retailers to put their payment networks into separate VLANs (scopes) from other non-sensitive data (out-of-scope).

Figure 5-92 shows an example of switch segmentation.

Figure 5-92 Cisco Store Switch Segmentation



Although the enforcement of these boundaries would be handled by either a router or firewall, the switch provides the port density and access required to connect the payment devices from the store floor.

Table 5-40 lists the component assessment details for the Cisco store switches.

Table 5-41 Component Capability Assessment—Store Switches

Store Switches	
PRIMARY FUNCTION	**Requirement 9, 11 (9.1.2, 11.1.b)**
Provide secure access to payment devices in the stores.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- The configurations of the Cisco Catalyst switches in the store architectures are maintained within EMC Ionix Network Configuration Manager (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- The use of VLANs on the Cisco Catalyst switch enables the retailer to provide same-box wired access to its devices while maintaining segregated addressing schemes.
- Disable the HTTP server on the switch and enable the HTTP secure server.
- Using the stacking capability of Cisco Catalyst switches improves high availability designs while simplifying configuration and support.
- Cisco SmartPorts simplifies connecting the right device to the right VLAN.
- Network Admission Control (NAC) protects the network from rogue devices being connected.
- Cisco compact switches can easily add more securely managed ports where needed (for example, Cash Wrap and customer service desk), and some models can use PoE.
- Set the **session** and **exec timeout** commands to 15 minutes or less.

- Configure appropriate banner messages on login, incoming, and exec modes of the switch. The login banner warning should not reveal the identity of the company that owns or manages the switch. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the switch to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the switch itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the switch.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco switches can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists.

  ```
  no ip http server
  ip http secure-server
  ip scp server enable
  snmp-server user remoteuser remoteuser v3
  line vty 0 4
   transport preferred none
   transport input ssh
   transport output none
  line vty 5 15
   transport preferred none
   transport input ssh
   transport output none
  ```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco switches may have several services that are enabled by default that can be disabled.

  ```
  no service pad
  no service udp-small-servers
  no service tcp-small-servers
  no service finger
  no ip http server
  ```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco switches support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

Note Strong cryptography—Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Before Crypto keys can be generated hostname and domain name must be entered

hostname S-A2-Small-1
ip domain name cisco-irn.com

! Generate keys with 1024 or larger bit key generation NOT the default 512

Crypto key generate rsa

ip ssh version 2

ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco switches. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

To meet all of the requirements listed below, the PCI solution for retail uses the centralized user database in Active Directory, which is linked to via LDAP, RADIUS, and TACACS+ services. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. This resource is used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco switches are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco switches, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

  Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

  These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco switches to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure ACS must be implemented. Configure AAA services as shown above in Requirement 7.

The switch is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

Cisco switches support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco switches require the setting of a password.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the switches also support the use of AES encryption of pre-shared keys.

  ```
  service password-encryption
  password encryption aes
  ```

  Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fallback user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco switches do not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco switches support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco switches support the local ability to block logins after a specified time after failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco switch management interfaces are configured as follows to meet this requirement:

  ```
  ip http timeout-policy idle 900

  line con 0
   session-timeout 15 output
   exec-timeout 15 0
  line vty 0 4
   session-timeout 15  output
   exec-timeout 15 0
  line vty 5 15
   session-timeout 15  output
   exec-timeout 15 0
  ```

Note If only the **session timeout** command is specified, the session timeout interval is based solely on detected input from the user. If the **session timeout** command is specified with the **output** keyword, the interval is based on both input and output traffic. You can specify a session timeout on each port. The **session-timeout** command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state. You can use a combination of the **exec-timeout** and **session-timeout** line configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the **session-timeout** command causes on physical lines.

Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.2**—*Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.*

  In addition to disabling switch port interfaces for ports that are not in use, or in public areas, ports can also be placed in the guest network VLAN. This VLAN is treated as a public network and requires the appropriate PCI requirements for public networks to be met as well (for example, IPS/IDS and stateful firewall). Cisco switches support a feature called SmartPorts, whereby devices connected to these ports can be dynamically moved to an appropriate network VLAN from a blackhole VLAN or guest VLAN based on automatic identification macros. This allows ports to be active for periodic use when devices are attached (for example, media players for in-aisle promotions, and IP phones for customer service) when these network ports are in publicly accessible areas. The following configurations show how to enable SmartPorts for a variety of default or custom devices based on MAC addresses as opposed to 802.1x authentication methods.

```
!
macro global description cisco-desktop
!
macro auto execute CISCO_LAST_RESORT_EVENT builtin CISCO_AP_AUTO_SMARTPORT
ACCESS_VLAN=17
macro auto execute Retail-POS builtin CISCO_PHONE_AUTO_SMARTPORT ACCESS_VLAN=11
VOICE_VLAN=13
macro auto execute POS-Systems remote scp://SMARTPORT@192.168.42.122/POS-Systems.txt
ACCESS_VLAN=11 VOICE_VLAN=13
!
macro auto mac-address-group Retail-POS
 oui list 001C26
 oui list 001C25
 mac-address list 0021.5C02.1DEF
 mac-address list 001C.25BE.99C2
macro auto device media-player ACCESS_VLAN=12
macro auto device ip-camera ACCESS_VLAN=20
macro auto device phone ACCESS_VLAN=17 VOICE_VLAN=13
macro auto device access-point ACCESS_VLAN=18
macro auto device lightweight-ap ACCESS_VLAN=18
!
macro auto global processing fallback cdp
!
interface GigabitEthernet0/9
 macro description CISCO_SWITCH_EVENT
```

More information about Cisco SmartPorts can be found at the following URL: http://www.cisco.com/en/US/docs/switches/lan/auto_smartports/12.2_55_se/configuration/guide/asp_cg.html

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events when using 802.1x.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*

  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco switches track individual administrator actions as identified in the requirement above (10.1, 10.2, and 10.3) through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

Cisco switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco switches use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

  To learn more about NTP, visit:
  http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Note The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

Requirement 11: Regularly Test Security Systems and Processes

The following requirements can be addressed using Cisco Network Admission Control.

- **PCI 11.1.b**—*Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:*
  - *WLAN cards inserted into system components*
  - *Portable wireless devices connected to system components (for example, by USB, etc.)*
  - *Wireless devices attached to a network port or network device*
- **PCI 11.1.d**—*If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.*

  Cisco NAC capabilities can be configured on the store switches to automate the verification of approved devices being attached to the network. In addition to configuring the NAC authentication services in the data center, add the following configurations to the switch and switch interface ports where NAC is to be used (for example, publicly accessible ports):

```
Pre-requirements for NAC (domain name, name server, time settings, crypto keys):
 ip domain-name cisco-irn.com
 ip name-server 192.168.42.130
 Crypto key generate rsa 1024
 ntp server 192.168.62.161 prefer
 ntp server 192.168.62.162
 clock timezone PST -8
 clock summer-time PDT recurring
!
! ----Configurations to add for NAC ----
!
aaa new-model
!
!
aaa authentication dot1x default group radius local
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 192.168.42.111
 server-key 7 <removed>
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 5 tries 3
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
radius-server vsa send accounting
radius-server vsa send authentication
!
authentication mac-move permit
!
!
ip device tracking
ip admission name ise proxy http inactivity-time 60
!
cts sxp enable
cts sxp default source-ip 10.10.111.13 {use Switch Management IP}
!
dot1x system-auth-control
!
fallback profile ise
 ip access-group ACL-DEFAULT in
 ip admission ise
!
! ----Auto Smart Ports Macro method for port configurations-------
!
macro name dot1x
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout tx-period 5
```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco Catalyst Switches—Data Center

The Cisco Catalyst family of data center switches securely switches data; from servers to high speed trunks, maintaining the integrity of segmented scopes of compliance. They provide scalable inter-switch connectivity, high port density for wired endpoints, and the ability to segment them into sensitive scope networks. VLANs are used to put sensitive PCI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks. Data center Cisco Catalyst switches are highly redundant, capable of delivering high performance switching, with feature options depending on the needs of the business.

Modular functionality provides the ability to insert security technology to enforce compliance needs.

- Security services include access control, firewall, and intrusion prevention.
- Wireless services can be aggregated into these switches for central policy control of unified wireless access points.
- Application services include quality of service (QoS), content filtering, and load balancing.

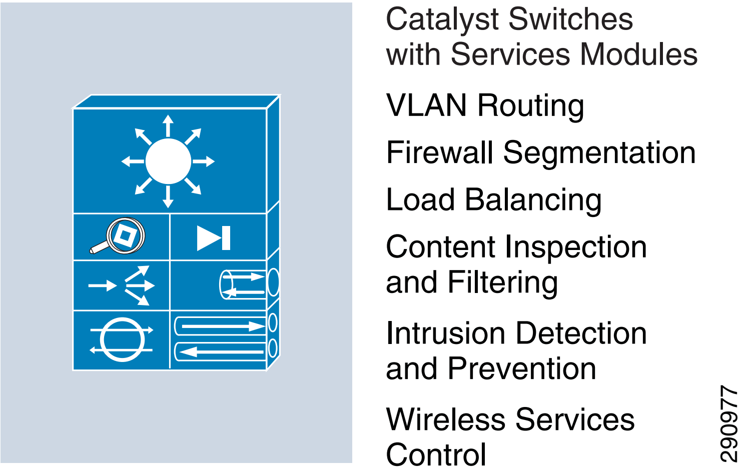
Table 5-42 PCI Assessment Summary—Cisco Catalyst Data Center Switches

Models Assessed	
Catalyst6509-Sup720-3BXL version s72033-adventerprisek9_wan-mz.122-33.SXJ.bin WS-C3750-48P version c3750-ipbasek9-mz.122-55.SE1.bin WS-C4948-10GE version cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin	
PCI Sub-Requirements Passed	
PCI 1	1.2.2
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 9	9.1.1
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary PCI compliance feature of Cisco Catalyst data center switches is securing the infrastructure. Cisco Catalyst switches have firewall/IDS modules for perimeter security. (See Figure 5-93.)

Figure 5-93 Cisco Catalyst Data Center Switches



The main function of the Cisco Catalyst data center switches is segmentation of PCI scope and enforcement of that new scope boundary. These switches have five primary functions/capabilities in relation to PCI:

- Using VLANs, Cisco Catalyst switches allow a retailer to put its payment networks into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Catalyst switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, a retailer can isolate sensitive information from non-sensitive information. The Cisco Catalyst switch can perform the ability to segment and route sensitive traffic from non-sensitive and reduce the overall scope of a company's cardholder data environment. Depending on risk vectors, different levels of enforcement are required at the segmented scope boundary level. See the following bullets for details.
- The Layer 3 Cisco Catalyst switch acts as a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network. A Cisco Catalyst switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the retailer. ACLs may not be used to segment untrusted networks.
- The Cisco Catalyst switch with a firewall service module restricts traffic between the cardholder data environment and other areas of the network. As soon as any untrusted network is introduced, firewalling and IDS/IPS must be deployed.
- The Layer 3 Cisco Catalyst switch with an intrusion prevention module inspects all traffic going to and from the cardholder data environment. As soon as any untrusted network is introduced, firewalling and IDS/IPS must be deployed.

Table 5-42 lists the component assessment details for the Cisco Catalyst data center switches.

Table 5-43 Component Capability Assessment—Cisco Catalyst Data Center Switches

Cisco Catalyst Data Center Switches	
PRIMARY FUNCTION	**Requirement 1, 11 (1.2, 1.3, 11.4)**
Provide secure access to payment infrastructure and servers using VLANs, ACLs, and firewall/IPS.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- The configurations of the Cisco Catalyst switches in the data center and Internet edge architectures are maintained within EMC Ionix Network Configuration Manager (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- The use of VLANs on the Cisco Catalyst switch enables the retailer to provide same-box wired access to its devices while maintaining segregated addressing schemes.
- Using the stacking capability of Cisco Catalyst switches improves high availability designs while simplifying configuration and support.
- Disable the HTTP server on the switch and enable the HTTP secure server.
- Set the **session** and **exec timeout** commands to 15 minutes or less.
- Configure appropriate banner messages on login, incoming, and exec modes of the switch. The login banner warning should not reveal the identity of the company that owns or manages the switch. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the switch to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the switch itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the switch.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Router and switch configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of routers and switches are synchronized.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco switches can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists.

```
no ip http server
ip http secure-server
ip scp server enable
snmp-server user remoteuser remoteuser v3
line vty 0 4
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
```

```
transport preferred none
transport input ssh
transport output none
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco switches may have several services that are enabled by default that can be disabled.

  ```
  no service pad
  no service udp-small-servers
  no service tcp-small-servers
  no service finger
  no ip http server
  ```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco switches support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco switches. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*

- **PCI 7.2.3**—*Default “deny-all” setting. Note: Some access control systems are set by default to “allow-all,” thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco switches are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco switches, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa new-model
    aaa authentication login RETAIL group tacacs+ local
    aaa authentication enable default group tacacs+ enable
    aaa authorization exec default group tacacs+ if-authenticated
    aaa accounting update newinfo
    aaa accounting exec default start-stop group tacacs+
    aaa accounting commands 15 default start-stop group tacacs+
    aaa accounting system default start-stop group tacacs+
    aaa session-id common
    tacacs-server host 192.168.42.131
    tacacs-server directed-request
    tacacs-server domain-stripping
    tacacs-server key 7 <removed>
```

  Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

  These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

The switch is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco switches support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

```
    username bart privilege 15 secret 5 <removed>
    username emc-ncm privilege 15 secret 5 <removed>
```

```
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco switches require setting of a password.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the switches also support the use of AES encryption of pre-shared keys.

  ```
  service password-encryption
  password encryption aes
  ```

  Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fall back user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco switches do not support the ability to specify a minimum password length for local accounts; this would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco switches support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco switches support the local ability to block logins after a specified time after failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco switch management interfaces are configured as follows to meet this requirement:

  ```
  ip http timeout-policy idle 900

  line con 0
   session-timeout 15 output
   exec-timeout 15 0
  line vty 0 4
   session-timeout 15  output
   exec-timeout 15 0
  line vty 5 15
   session-timeout 15  output
   exec-timeout 15 0
  ```

Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.1**—*Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events when using 802.1x.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*

- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco switches track individual administrator actions as identified in the requirement above (10.1, 10.2, and 10.3) through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

Cisco switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco switches use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

  To learn more about NTP, visit:
  http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Note The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco Nexus 1000V Switch—Data Center

The Cisco Nexus 1000V Series Switch provides connectivity for virtual servers with the ability to segment them onto their own sensitive scope networks. VLANs are used to put sensitive PCI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks.

The Cisco Nexus 1000V Series Switch provides advanced networking functions and a common network management model in a virtualized server environment. The Cisco Nexus 1000V Series Switch replaces the virtual switching functionality of the VMware vCenter data center container of servers. Each server in the data center container is represented as a line card in the Cisco Nexus 1000V Series Virtual Supervisor Module (VSM) and is managed as if it were a line card in a physical Cisco switch.

Key benefits of the Nexus 1000V include the following:

- Policy-based virtual machine (VM) connectivity
- Mobile VM security and network policy
- Non-disruptive operational model for your server virtualization, and networking teams

Table 5-44 PCI Assessment Summary—Cisco Nexus 1000V Series Switch

Models Assessed	
Cisco Nexus 1000V version 4.2(1)SV1(4)	
PCI Sub-Requirements Passed	
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10. 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	

Table 5-44 PCI Assessment Summary—Cisco Nexus 1000V Series Switch (continued)

PCI Sub-Requirements Failed
No sub-requirements were failed.

Primary PCI Function

The primary PCI compliance feature of Cisco Nexus switches is secure aggregation and access layer connectivity.

- Using VLANs, Cisco Nexus switches allow a retailer to put its payment network into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Nexus switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, a retailer can isolate sensitive information from non-sensitive information. The Cisco Nexus switch can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's cardholder data environment. Depending on risk vectors, various levels of enforcement are required at the segmented scope boundary level.
- The Layer 3 Cisco Nexus switch acts as a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network. A Cisco Nexus switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the retailer. ACLs may not be used to segment untrusted networks.
- The Cisco Nexus switch uses *virtualization contexts*, which are essentially virtualized switches. Each virtualized context has its own configuration and management interfaces that can be used to segregate not only data but administration as well.

Table 5-44 lists the component assessment details for the Cisco Nexus 1000V Series Switch.

Table 5-45 Component Capability Assessment—Cisco Nexus 1000V Series Switch

Cisco Nexus 1000V Series Switch	
PRIMARY FUNCTION	**Requirement 1**
Secure aggregation and access layer connectivity.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

The Cisco Nexus 1000V Series Switch includes the Cisco Integrated Security features that are found on Cisco physical switches to prevent a variety of attack scenarios. For example, a rogue virtual machine can spoof its MAC and IP addresses so that it appears to be an existing production virtual machine, send a rogue Address Resolution Protocol (ARP) transaction mimicking the way that VMware vMotion announces the location of a migrated virtual machine, and divert traffic from the production virtual machine to the rogue virtual machine. With Cisco Integrated Security features, this type of attack can easily be prevented with simple networking policy. Because server virtualization is being used for desktop and server workloads, it is critical that this type of security feature be deployed for the proper operation of a virtualized environment.

The Cisco Nexus 1000V Series implementation has two main components:

- Virtual Supervisor Module (VSM)
- Virtual Ethernet module (VEM)

The Cisco Nexus 1000V VSM is installed as an appliance server on either a standalone Cisco UCS server (Cisco Nexus 1010) or as a virtual appliance on VMware ESXi server running on a blade of the Cisco UCS system.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  On the Cisco Nexus 1000V, you can turn off the unwanted services such as Telnet and HTTP.

  ```
  no feature http-server
  no feature telnet
  ```

  The remote access is restricted to SSH when you turn off the Telnet service.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  Cisco SMARTnet services provide ongoing access to software updates and security patches. Cisco Nexus 1000V update software includes fixes for security vulnerabilities along with other bug fixes. The software is available directly from the Cisco website.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database. It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel’s job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*

- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  TACACS+ provides for separate authentication, authorization, and accounting services. The TACACS+ daemon provides each service independently.

  First, you have to enable the TACACS+ feature on the Cisco Nexus 1000V:

  ```
  config t
  feature tacacs+
  ```

  The following commands show how to configure the TACACS+ server:

  ```
  tacacs-server key 7 password
  tacacs-server host 192.168.42.131
  aaa group server tacacs+ CiscoACS
      server 192.168.42.131
      use-vrf management
      source-interface mgmt0
  aaa group server tacacs+ tacacs
  aaa authentication login default group CiscoACS
  ```

  Number *7* in the key command specifies an encrypted string (key) to follow.

  Local is the default and is used when no methods are configured or when all the configured methods fail to respond. Configure the local user with encrypted passwords for fallback authentication:

  ```
  username admin password 5 <removed>  role network-admin
  username retail password 5 <removed>  role network-operator
  ```

  Both roles used in the **username** commands are pre-defined roles in the Cisco Nexus 1000V. The network admin role has access to all commands on the switch, whereas the network operator role has access to all read commands on the switch.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters. PCI Sub-Requirements with Compensating Controls*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Nexus Switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco Nexus switches track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

  ```
  logging server 192.178.42.124 6 facility syslog

  aaa accounting default group CiscoACS
  ```

Cisco Nexus switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco Nexus switches use NTP to meet these requirements by implementing the following configuration statements.

```
enable NTP
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management

clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
```

To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco Nexus Switches—Data Center

The Cisco Nexus family of data center switches securely switches data; from payment application servers to high speed trunks of the core, maintaining the integrity of segmented scopes of compliance. They provide scalable inter-switch connectivity and high port density for wired endpoints. VLANs are used to put sensitive PCI applications and devices onto their own network and segregate them from devices on non-sensitive networks.

Cisco Nexus switches are ideal for enterprise-class server and aggregation layer deployments. These multipurpose, multilayer switches can be deployed across a diverse set of traditional, virtualized, unified, and high-performance computing environments. They enable diverse transports over Ethernet (including Layer 2, Layer 3, and storage traffic) on one common platform. Nexus switches help transform your data center, with a standards-based, multipurpose, multiprotocol, Ethernet-based fabric.

Table 5-46 PCI Assessment Summary—Cisco Nexus Data Center Switches

Models Assessed	
Cisco Nexus5020 Chassis (“40x10GE/Supervisor”) version n5000-uk9.5.0.3.N1.1b.bin Cisco 7010 Chassis (“Supervisor module-1X”) version n7000-s1-dk9.5.1.2.bin	
PCI Sub-Requirements Passed	
PCI 1	1.2.2

Table 5-46 PCI Assessment Summary—Cisco Nexus Data Center Switches (continued)

PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10. 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary PCI compliance feature of Cisco Nexus data center switches is secure aggregation and access layer connectivity.

- Using VLANs, Cisco Nexus switches allow a retailer to put its payment network into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Nexus switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, a retailer can isolate sensitive information from non-sensitive information. The Cisco Nexus switch can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company’s cardholder data environment. Depending on risk vectors, various levels of enforcement are required at the segmented scope boundary level.
- The Layer 3 Cisco Nexus switch acts as a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network. A Cisco Nexus switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the retailer. ACLs may not be used to segment untrusted networks.
- The Cisco Nexus switch uses virtualization contexts, which are essentially virtualized switches. Each virtualized context has its own configuration and management interfaces that can be used to segregate not only data but administration as well.

Table 5-46 lists the component assessment details for the Cisco Nexus data center switches.

Table 5-47 Component Capability Assessment —Cisco Nexus Data Center Switches

Cisco Nexus Data Center Switches	
PRIMARY FUNCTION	**Requirement 1 (1.3.5)**
Secure access to payment infrastructure and servers using segmentation of trusted networks (VLANs, ACLs).	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- Configuration was done manually on the router CLI, and backup of configuration and monitoring of configuration for changes and non-compliance were done through the EMC Ionix Network Configuration Manager (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- Configure appropriate banner messages on login, incoming, and EXEC modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Nexus switches in the data center were implemented using guidance from the Enterprise Data Center Design guide based on a Data Center 3.0 Architecture:
  http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html

  Enterprise Internet Edge Design Guide:
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html
- The Cisco Nexus 7010 and the Cisco Nexus 5000 were used for the aggregation block portions of the lab validation network.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Cisco Nexus configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations are synchronized.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco Nexus switches can be configured to use secure protocols for all system functions. This includes SSH for remote management, SCP, and SFTP for file transfers. Insecure services can be disable or blocked using configuration statements and access lists.

  ```
  no feature telnet
  no telnet server enable
  feature ssh
  ```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Nexus switches have no extraneous services that are enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco Nexus switches support administrative protocols with strong cryptography such as SSH version 2.

Note Strong cryptography—Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Generate keys with 1024 or larger bit key generation NOT the default 512

ssh key rsa 1024 force

! Cisco Nexus switches utilize SSH version 2.
```

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

Cisco SMARTnet services provide ongoing access to software updates and security patches: http://www.cisco.com/cisco/software/type.html?mdfid=282099479&flowid=3088.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco Nexus switches are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels have access to only the information they require for their job function. By default in Cisco Nexus switches, no users are allowed access unless specifically configured and assigned.

```
feature tacacs+

aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
```

Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username admin password 5 <removed>  role network-admin
username retail password 5 <removed>  role network-admin
username bart password 5 <removed>  role network-admin
username emc-ncm password 5 <removed>  role network-admin
```

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco Nexus switches to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure Access Control Server must be implemented. Configure AAA services as shown above in Requirement 7.

The switch is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco Nexus switches support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts. They should be individually unique as specified by policy.

  ```
  username admin password 5 <removed>  role network-admin
  username retail password 5 <removed>  role network-admin
  username bart password 5 <removed>  role network-admin
  username emc-ncm password 5 <removed>  role network-admin
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*

  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco Nexus switches support the ability to specify a password.

  ```
  username admin password 5 <removed>  role network-admin
  username retail password 5 <removed>  role network-admin
  username bart password 5 <removed>  role network-admin
  username emc-ncm password 5 <removed>  role network-admin
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Local user fall back accounts are created with the **username** command and use MD5-encryption for the user password. Communication to the AAA server using RADIUS or TACACS+ is encrypted when using centralized authentication.

  ```
      username admin password 5 <removed>  role network-admin
      username retail password 5 <removed>  role network-admin
      username bart password 5 <removed>  role network-admin
      username emc-ncm password 5 <removed>  role network-admin
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco Nexus switches do not support an automated capability to perform this function at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco Nexus switches do not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

Requirements 8.5.10–8.5.11 can be satisfied with a single configuration statement as identified below.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.PCI Sub-Requirements with Compensating Controls*

  The NX-OS software accepts only strong passwords when you have password strength checking enabled (default) using the **password strength-check** command. The characteristics of a strong password include the following:

  - At least eight characters long
  - Does not contain many consecutive characters (such as "abcd")
  - Does not contain many repeating characters (such as "aaabbb")
  - Does not contain dictionary words
  - Does not contain proper names
  - Contains both uppercase and lowercase characters
  - Contains numbers

  ```
  password strength-check
  ```

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco Nexus switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco Nexus switches do not support the ability to lock out local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco Nexus switches do not support the ability to manage lockout of local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco Nexus switch management interfaces are configured as follows to meet this requirement:

  ```
  line console
    exec-timeout 15

  line vty
    exec-timeout 15
  ```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Nexus switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*

  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco Nexus switches track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging server 192.168.42.124 6
!
! --- for implementations using VRF's ----
!
logging server 192.168.42.124 6 use-vrf servers1

aaa accounting default group CiscoACS
```

Cisco Nexus switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco Nexus switches use NTP to meet these requirements by implementing the following configuration statements.

```
! NTP can only be configured in the default VDC
!
enable NTP
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management

clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
```

  To learn more about NTP, visit:
  http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Wireless

Cisco Wireless technologies provide connectivity for mobile clients within the store. They can secure connectivity for traditional business functions such as guest access or inventory control, without increasing risk. Innovative customer experience services such as mobile point-of-sale are equally secure. In addition to expanding business functionality, Cisco wireless technology seamlessly provides the capability to detect rogues.

Industry-leading performance is available with Cisco Aironet access points for highly secure and reliable wireless connections for both indoor and outdoor environments. Cisco offers a broad portfolio of access points targeted to specific business needs and topologies.

Cisco wireless controllers help reduce the overall operational expenses of Cisco Unified Wireless Networks by simplifying network deployment, operations, and management. They extend the Cisco Borderless Network policy and security from the wired network to the wireless edge.

Cisco Wireless Control System (WCS) delivers full visibility and control of Cisco Aironet access points, Cisco Wireless LAN Controllers (WLC) and the Cisco Mobility Services Engine (MSE) with built-in support for Cisco adaptive wireless intrusion prevention systems (wIPS) and Cisco context-aware services. This robust platform helps you reduce total cost of ownership and maintain a business-ready wireless network.

Table 5-48 PCI Assessment Summary—Cisco Wireless Products

Models Assessed	
AIR-CT5508-12-K9 version 7.0.114.112 MSE3550 version 7.0.200.125 Cisco WCS Manager version 7.0.171.107 AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N	
PCI Sub-Requirements Passed	
PCI 2	2.1.1, 2.2, 2.2.2, 2.2.4, 2.3

Table 5-48 PCI Assessment Summary—Cisco Wireless Products (continued)

PCI 4	4.1, 4.1.1
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI 11	11.1.b, 11.1.d
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary PCI function of Cisco Unified Wireless is secure connectivity of wireless clients (4.1) and rogue detection (1.1).

Table 5-48 lists the component assessment details for Cisco wireless products.

Table 5-49 Component Capability Assessment —Cisco Wireless Products

Cisco Wireless Products	
PRIMARY FUNCTION	**Requirement 4, 11 (4.1, 11.1)**
Secure access to payment infrastructure and servers using segmentation of trusted networks (VLANs, ACLs).	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

Rogue detection for wireless technology in the store is required at a minimum of once a quarter, whether or not the retailer has wireless deployed. A hacker might infiltrate a store and install a rogue wireless device (for example, access point, wireless-enabled printer, or radio-enabled USB stick). This would allow a hacker remote access into the store (from the parking lot, for example) that is hard to detect. The PCI DSS offers several methods for detecting rogue devices. Cisco Unified Wireless offers the benefit of continuous rogue detection while simultaneously passing normal wireless traffic.

The PCI-DSS states that wireless technology is an untrusted network connection. Wireless technology in the store requires firewall and intrusion detection services to segment and protect the cardholder data environment. Stateful firewalls must be configured to limit traffic to and from the wireless environment (all enabled services, protocols, and ports must have documented justification for business purposes). All other access must be denied.

When including point-of-sale clients in the wireless network, strong wireless encryption technology needs to be implemented.

Caution Wireless clients must be protected from each other, as well. For example, when using hand-held scanners and mobile POS, the scanners need to be on separate SSIDs and networks from the POS, and protected with firewall and intrusion detection services that are restricted to justified business access.

Wireless compliance is broken into the stages listed in Table 5-50.

Table 5-50 Wireless Compliance Stages

Wireless Deployment	Risk	Required Measure
No wireless deployed	Hacker deploys wireless into store	Rogue detection
Wireless deployed, no wireless POS/CDE	Hacker deploys unknown wireless into store, or hacks into existing wireless	Rogue detection Stateful firewall separating wired from wireless LAN Intrusion Detection System
Wireless deployed, includes wireless POS/CDE	Hacker deploys unknown wireless into store, or hacks into existing wireless	Rogue detection Stateful firewall separating wired from wireless LAN Intrusion Detection System Strong wireless encryption for CDE (e.g., WPA2) Wireless CDE must be protected from other wireless and wired segments using a stateful firewall (Req. 1,2,3)

Cisco recommends using the Unified Wireless (controller-based) architecture for retail wireless deployments because of the Cisco ongoing wireless strategy. The autonomous Cisco IOS access points are not being enhanced. Future security and user enhancements will be developed on the controller-based architecture.

For WCS servers running software versions prior to 4.1, Cisco recommends a combination of documented password policies, manual audit procedures, and firewall segmentation for WCS servers within the data center.

- Configure unique SSIDs
- Disable broadcast of the SSIDs

PCI Assessment Detail—PCI Sub-Requirements Satisfied

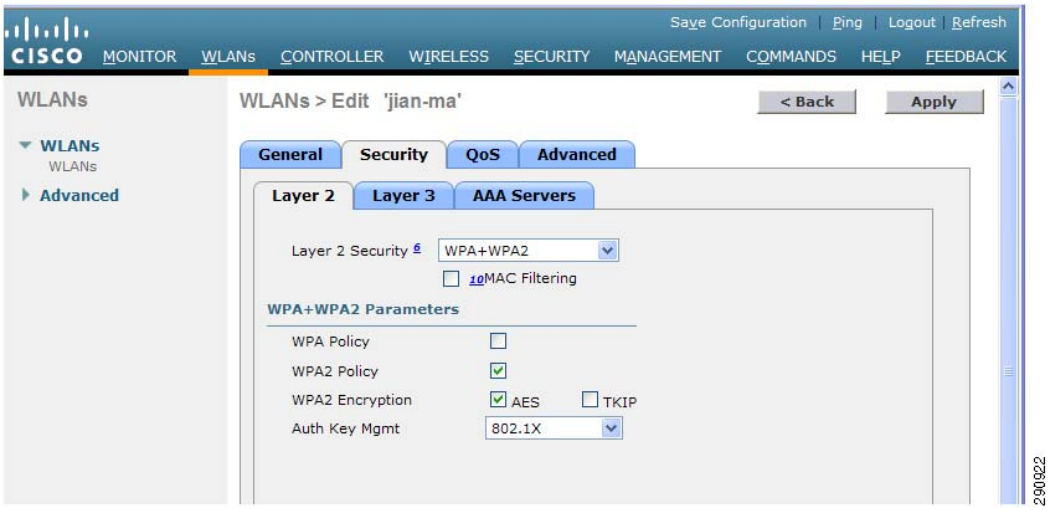
Whenever possible, a screenshot highlighting the appropriate Cisco Wireless Control System functionality is provided.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1.1**—*For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.*

  The Cisco Unified Wireless Network supports both Wi-Fi Protected Access (WPA) and WPA2 and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption (see Figure 5-94 and Figure 5-95). There is no default PSK, and all PSKs must be created during configuration. The Cisco Unified Wireless Network architecture does not use SNMP at the access points.

Figure 5-94 WLANs Security Screen



WLANs > Edit 'jian-ma'

Layer 2 Security 6 WPA+WPA2

□ 10MAC Filtering

WPA+WPA2 Parameters

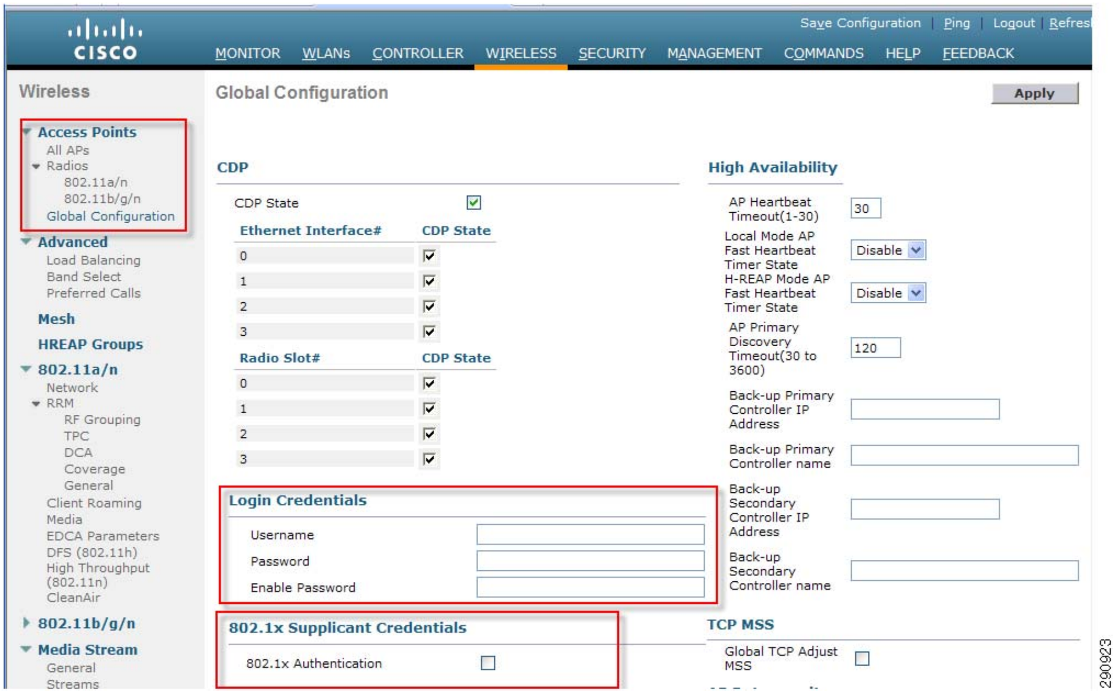
WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

Auth Key Mgmt 802.1X

Figure 5-95 Wireless Global Configuration Screen



Global Configuration

CDP

CDP State ☑

Ethernet Interface#	CDP State
0	☑
1	☑
2	☑
3	☑

Radio Slot#	CDP State
0	☑
1	☑
2	☑
3	☑

Login Credentials

Username	
Password	
Enable Password	

802.1x Supplicant Credentials

802.1x Authentication □

High Availability

AP Heartbeat Timeout(1-30)	30
Local Mode AP Fast Heartbeat Timer State	Disable
H-REAP Mode AP Fast Heartbeat Timer State	Disable
AP Primary Discovery Timeout(30 to 3600)	120
Back-up Primary Controller IP Address	
Back-up Primary Controller name	
Back-up Secondary Controller IP Address	
Back-up Secondary Controller name	

TCP MSS

Global TCP Adjust MSS □

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are no unnecessary services enabled by default on the Cisco Unified Wireless Control Server system. Cisco Unified Wireless Control Server should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository.

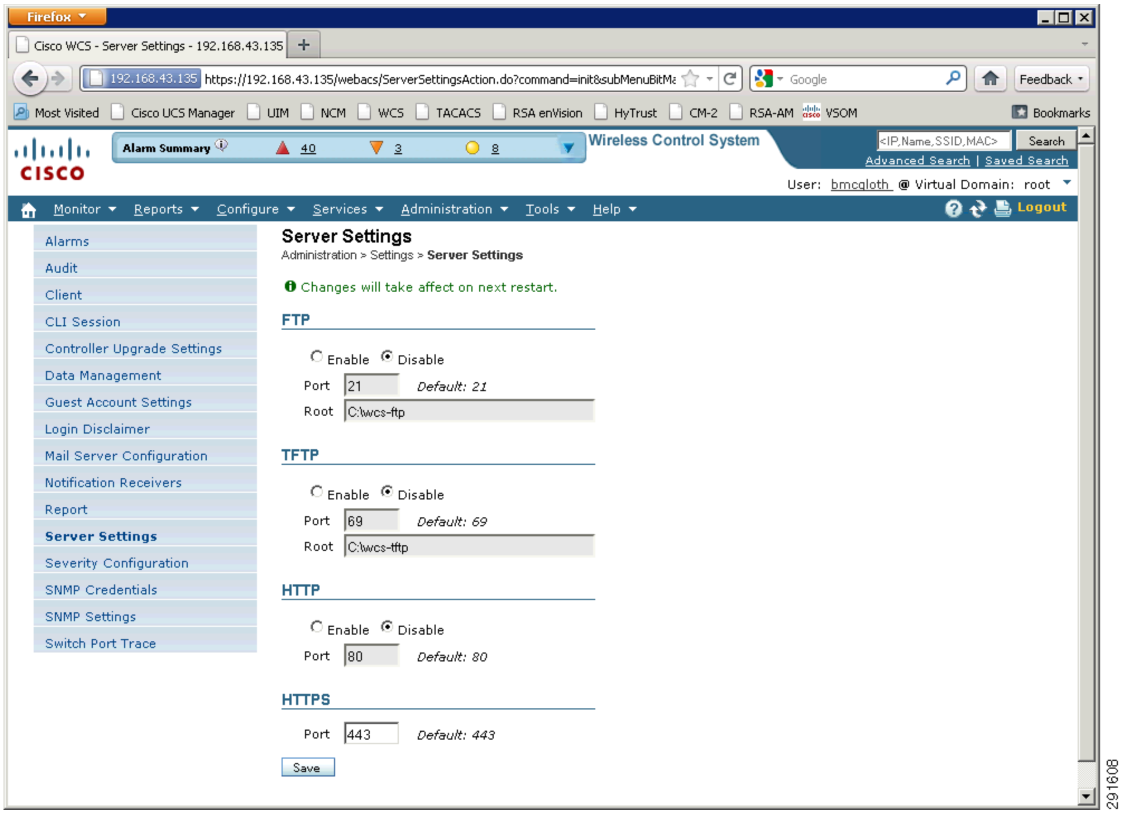
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers*

  Cisco Unified Wireless Control Server system should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

  Cisco Unified Wireless Control Server system can be configured for secure management using strong cryptography. Figure 5-96, Figure 5-97, Figure 5-98, and Figure 5-99 show where to disable non-encrypted management interfaces (for example, Telnet and HTTP).

Figure 5-96 WCS Server Secure Management


Firefox
Cisco WCS - Server Settings - 192.168.43.135
192.168.43.135 https://192.168.43.135/webacs/ServerSettingsAction.do?command=init&subMenuBitMa
Google
Feedback
Most Visited | Cisco UCS Manager | UIM | NCM | WCS | TACACS | RSA enVision | HyTrust | CM-2 | RSA-AM | VSOM | Bookmarks
CISCO
Alarm Summary 40 3 8
Wireless Control System
<IP,Name,SSID,MAC> Search
Advanced Search | Saved Search
User: bmcgloth @ Virtual Domain: root
Monitor | Reports | Configure | Services | Administration | Tools | Help | Logout
Alarms
Audit
Client
CLI Session
Controller Upgrade Settings
Data Management
Guest Account Settings
Login Disclaimer
Mail Server Configuration
Notification Receivers
Report
Server Settings
Severity Configuration
SNMP Credentials
SNMP Settings
Switch Port Trace
291608

Server Settings

Administration > Settings > **Server Settings**

Changes will take affect on next restart.

FTP

○ Enable ● Disable

Port 21 Default: 21

Root C:\wcs-ftp

TFTP

○ Enable ● Disable

Port 69 Default: 69

Root C:\wcs-tftp

HTTP

○ Enable ● Disable

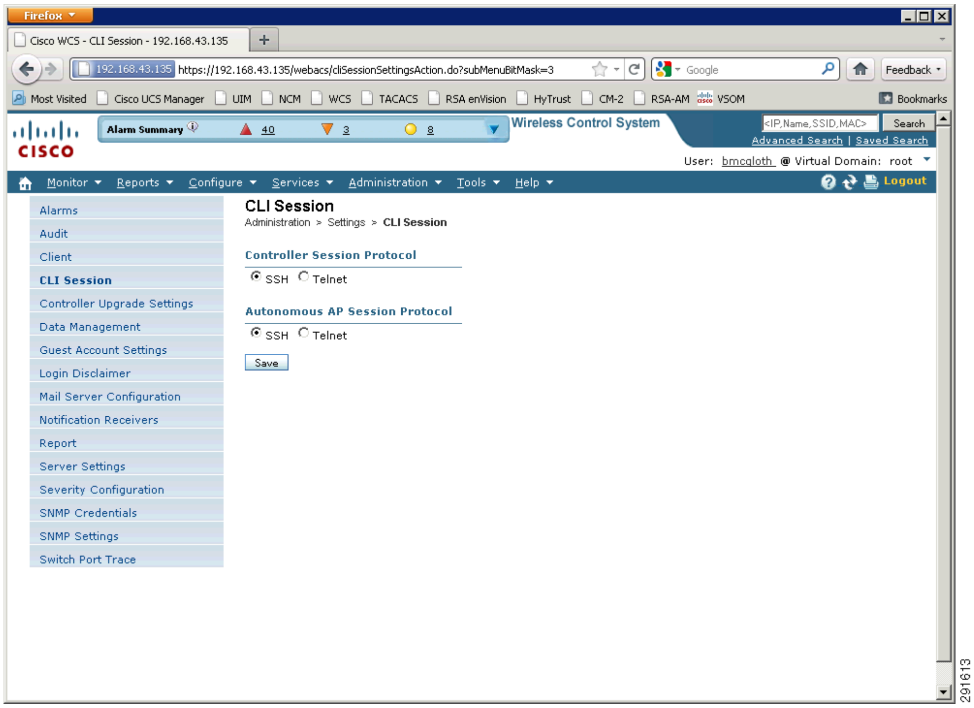
Port 80 Default: 80

HTTPS

Port 443 Default: 443

Save

Figure 5-97 CLI Session Secure Management


Firefox
Cisco WCS - CLI Session - 192.168.43.135
192.168.43.135 https://192.168.43.135/webacs/cliSessionSettingsAction.do?subMenuBitMask=3
Google
Feedback
Most Visited | Cisco UCS Manager | UIM | NCM | WCS | TACACS | RSA enVision | HyTrust | CM-2 | RSA-AM | VSOM | Bookmarks
CISCO
Alarm Summary 40 3 8
Wireless Control System
<IP,Name,SSID,MAC> Search
Advanced Search | Saved Search
User: bmcgloth @ Virtual Domain: root
Monitor | Reports | Configure | Services | Administration | Tools | Help | Logout
Alarms
Audit
Client
CLI Session
Controller Upgrade Settings
Data Management
Guest Account Settings
Login Disclaimer
Mail Server Configuration
Notification Receivers
Report
Server Settings
Severity Configuration
SNMP Credentials
SNMP Settings
Switch Port Trace
291613

CLI Session

Administration > Settings > **CLI Session**

Controller Session Protocol

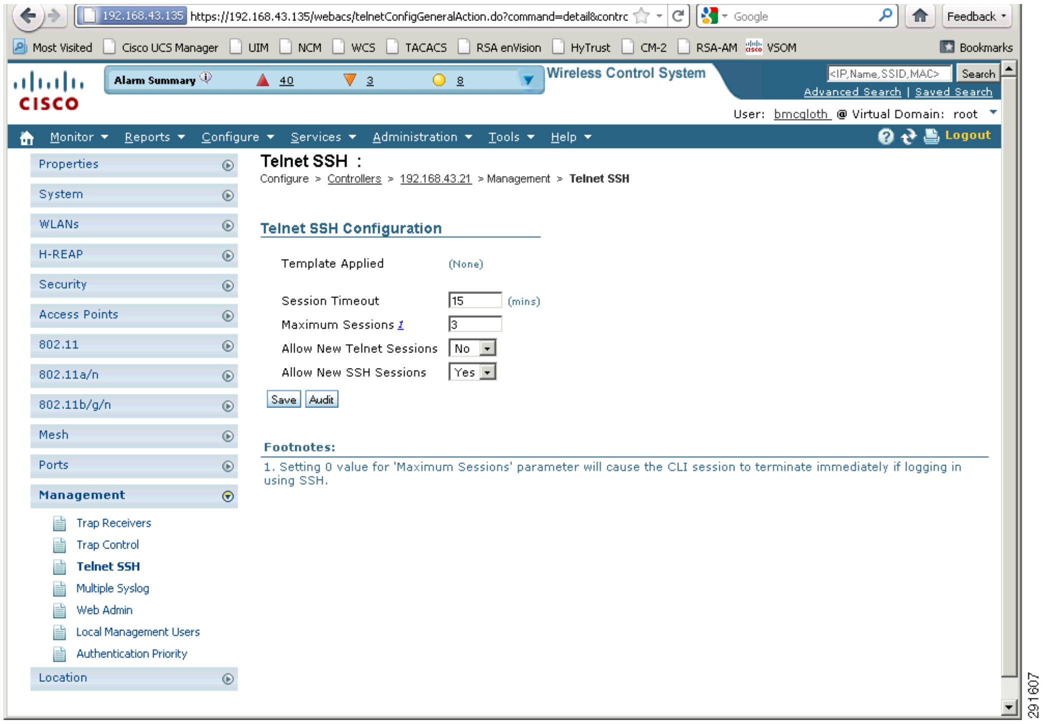
● SSH ○ Telnet

Autonomous AP Session Protocol

● SSH ○ Telnet

Save

Figure 5-98 Controller Secure Management for SSH



Telnet SSH :

Configure > Controllers > 192.168.43.21 > Management > Telnet SSH

Telnet SSH Configuration

Template Applied (None)

Session Timeout 15 (mins)

Maximum Sessions 1 3

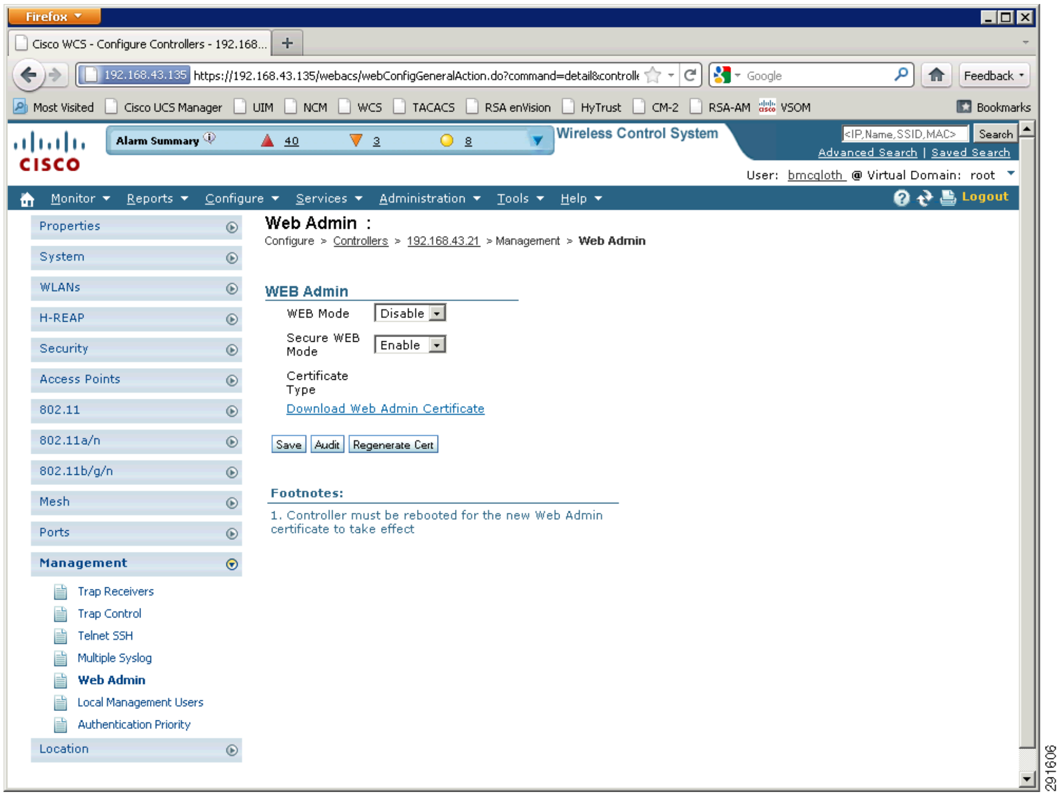
Allow New Telnet Sessions No

Allow New SSH Sessions Yes

Footnotes:

1. Setting 0 value for 'Maximum Sessions' parameter will cause the CLI session to terminate immediately if logging in using SSH.

Figure 5-99 Controller Secure Management for HTTPS



Web Admin :

Configure > Controllers > 192.168.43.21 > Management > Web Admin

WEB Admin

WEB Mode Disable

Secure WEB Mode Enable

Certificate Type

Download Web Admin Certificate

Footnotes:

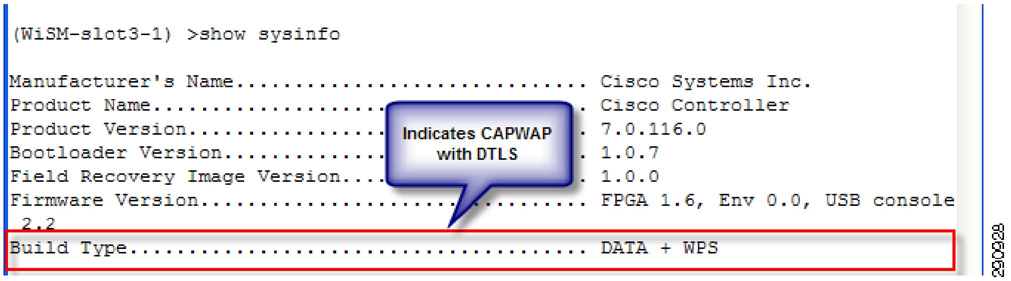
1. Controller must be rebooted for the new Web Admin certificate to take effect

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

  Cisco offers Control and Provisioning of Wireless Access Points (CAPWAP)-compliant DTLS encryption to ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links (see Figure 5-100). The Cisco Unified Wireless Network defaults to the highest CipherSuite available on the network. Furthermore, fallback on less secure SSL versions (that is, SSLv2 and SSLv1) can also be disabled, thus always forcing use of SSLv3. The Cisco Unified Wireless Network provides 256-bit encryption and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations.

Figure 5-100 CAPWAP with DTLS



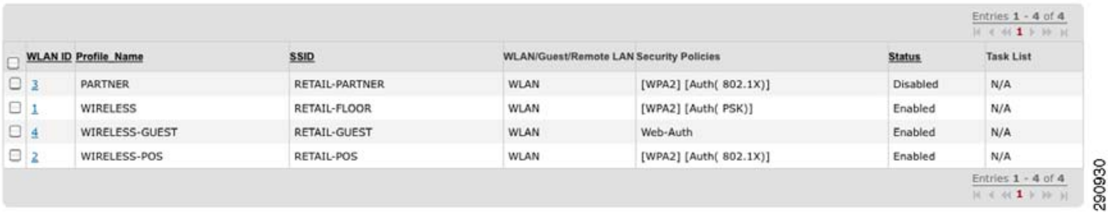
```
(WiSM-slot3-1) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name...................                 . Cisco Controller
Product Version................                 . 7.0.116.0
Bootloader Version.............                 . 1.0.7
Field Recovery Image Version...                 . 1.0.0
Firmware Version......................  ......... FPGA 1.6, Env 0.0, USB console
 2.2
Build Type....................................... DATA + WPS
```

- **PCI 4.1.1**—*Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Note: The use of WEP as a security control was prohibited as of 30 June 2010.*

  Cisco supports both WPA and WPA2 and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption. Cisco does not advertise the organization's name in the Service Set ID (SSID) broadcast. Cisco also disables SSID broadcast by default for non-guest networks. Cisco supports WPA2 Personal mode with a minimum 13-character random pass-phrase and Advanced Encryption Standard (AES) encryption, and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations. (See Figure 5-101.)

Figure 5-101 WLAN Information



Entries 1 - 4 of 4

□	WLAN ID	Profile_Name	SSID	WLAN/Guest/Remote LAN	Security Policies	Status	Task List
□	3	PARTNER	RETAIL-PARTNER	WLAN	[WPA2] [Auth(802.1X)]	Disabled	N/A
□	1	WIRELESS	RETAIL-FLOOR	WLAN	[WPA2] [Auth(PSK)]	Enabled	N/A
□	4	WIRELESS-GUEST	RETAIL-GUEST	WLAN	Web-Auth	Enabled	N/A
□	2	WIRELESS-POS	RETAIL-POS	WLAN	[WPA2] [Auth(802.1X)]	Enabled	N/A

Entries 1 - 4 of 4

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Unified Wireless. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS using TACACS+ and RADIUS services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

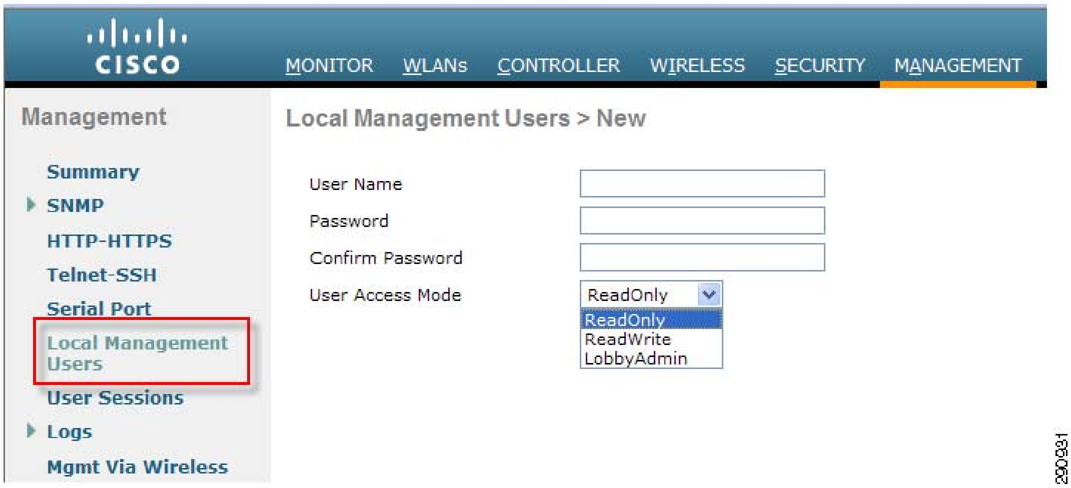
- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

Cisco Unified Wireless allows the network administrator to set user IDs that can be monitored and restricted with respect to access and other privileges when necessary.

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  The Cisco solution uses profiles where a user is assigned to the profile to ensure appropriate access to ensure network security, and user access can be restricted as shown in Figure 5-102 and Figure 5-103.

Figure 5-102 Local Management Users Screen



Local Management Users > New

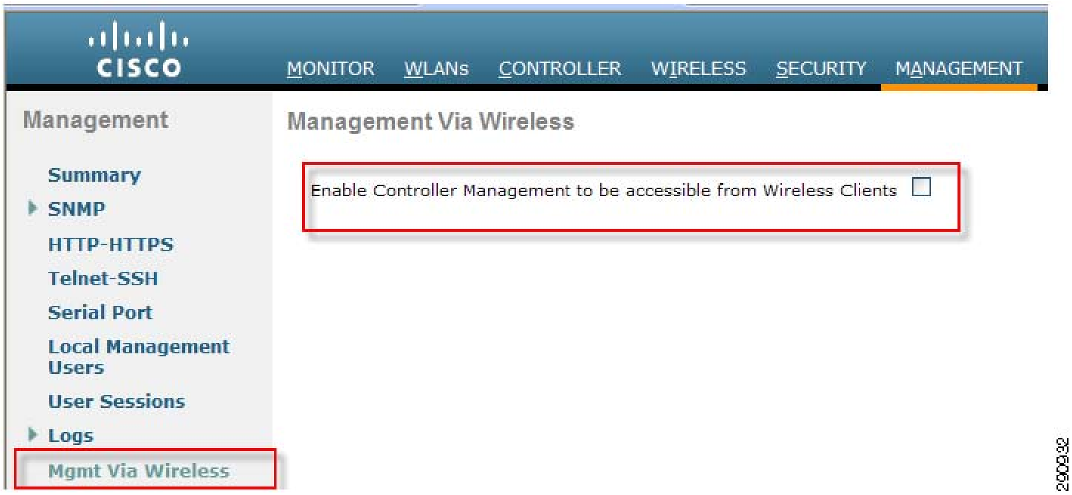
User Name

Password

Confirm Password

User Access Mode: ReadOnly
- ReadOnly
- ReadWrite
- LobbyAdmin

Figure 5-103 Management Via Wireless Screen

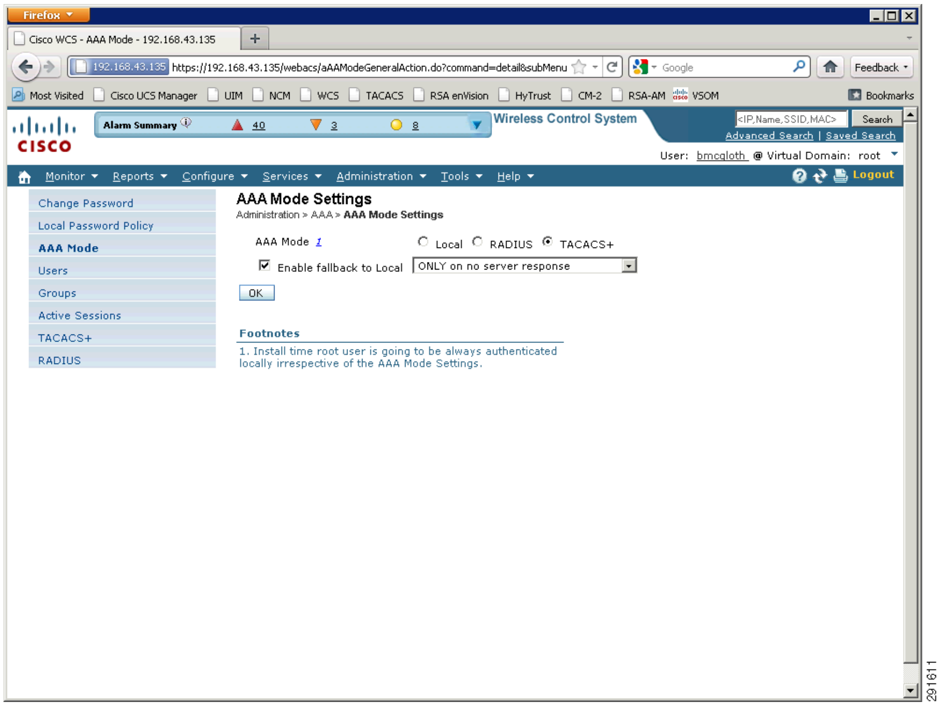


Management Via Wireless

Enable Controller Management to be accessible from Wireless Clients □

Cisco WCS is configured to use TACACS+ for authentication of administrators, as shown in Figure 5-104.

Figure 5-104 WCS Manager AAA Authentication Mode



AAA Mode Settings

Administration > AAA > **AAA Mode Settings**

AAA Mode 1 ○ Local ○ RADIUS ● TACACS+

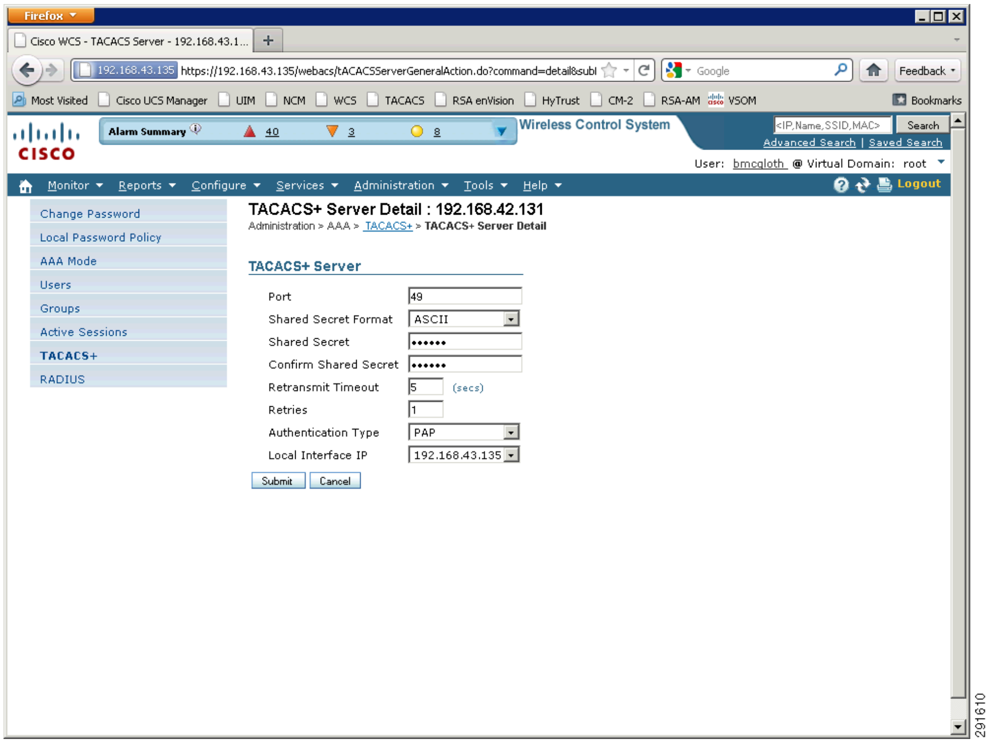
☑ Enable fallback to Local ONLY on no server response

Footnotes

1. Install time root user is going to be always authenticated locally irrespective of the AAA Mode Settings.

The authentication servers for TACACS+ in WCS Manager are configured as shown in Figure 5-105.

Figure 5-105 WCS Manager TACACS+ Server Configuration



TACACS+ Server Detail : 192.168.42.131

Administration > AAA > TACACS+ > **TACACS+ Server Detail**

TACACS+ Server

Port	49
Shared Secret Format	ASCII
Shared Secret	••••••
Confirm Shared Secret	••••••
Retransmit Timeout	5 (secs)
Retries	1
Authentication Type	PAP
Local Interface IP	192.168.43.135

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

Cisco Unified Wireless is able to meet some of the requirements locally, as identified below.

- **PCI 8.1**—Assign all users a unique ID before allowing them to access system components or cardholder data.

  Cisco WCS supports the creation of local user accounts with unique IDs. These can be used for local fallback user accounts. They should be individually unique as specified by policy.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco WCS Manager and controllers support the ability to specify a password.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Local user fall back accounts use MD5-encryption for the user password. Communication to the AAA server using RADIUS or TACACS+ is encrypted when using centralized authentication.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

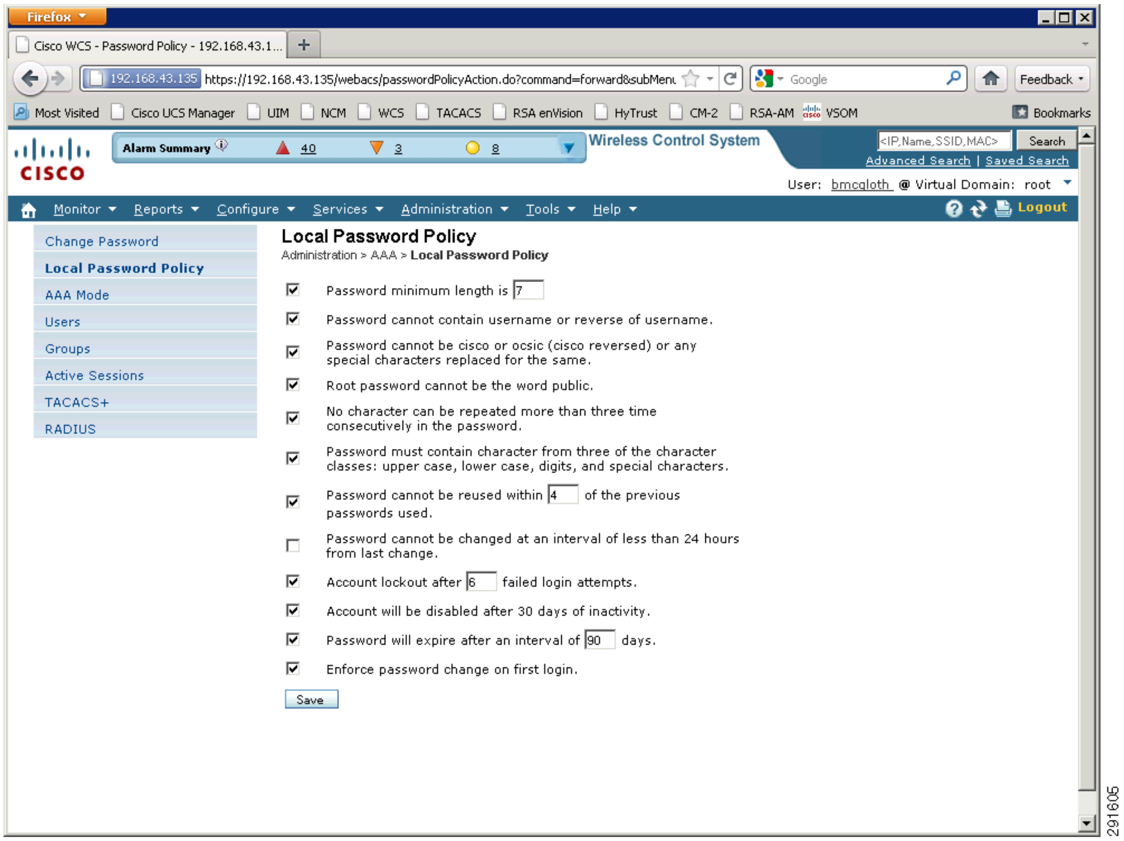
  Cisco Unified Wireless does not support an automated capability to perform this function at this time, user account would have to be manually reviewed in the device configurations every 90 days.

  The next several requirements (8.5.9–8.5.14) are addressed with the local password policy.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Figure 5-106 shows the local password policy that has been modified to meet the minimum requirements as specified by the preceding requirements.

Figure 5-106 WCS Manager Local Password Policy



Local Password Policy

Administration > AAA > Local Password Policy

☑ Password minimum length is 7

☑ Password cannot contain username or reverse of username.

☑ Password cannot be cisco or ocsic (cisco reversed) or any special characters replaced for the same.

☑ Root password cannot be the word public.

☑ No character can be repeated more than three time consecutively in the password.

☑ Password must contain character from three of the character classes: upper case, lower case, digits, and special characters.

☑ Password cannot be reused within 4 of the previous passwords used.

□ Password cannot be changed at an interval of less than 24 hours from last change.

☑ Account lockout after 6 failed login attempts.

☑ Account will be disabled after 30 days of inactivity.

☑ Password will expire after an interval of 90 days.

☑ Enforce password change on first login.

Save

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to reactivate the terminal or session.*

  Cisco WCS Manager limits sessions, as shown in Figure 5-98 above.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco Unified Wireless system is able to track and monitor all administrative user access and events.

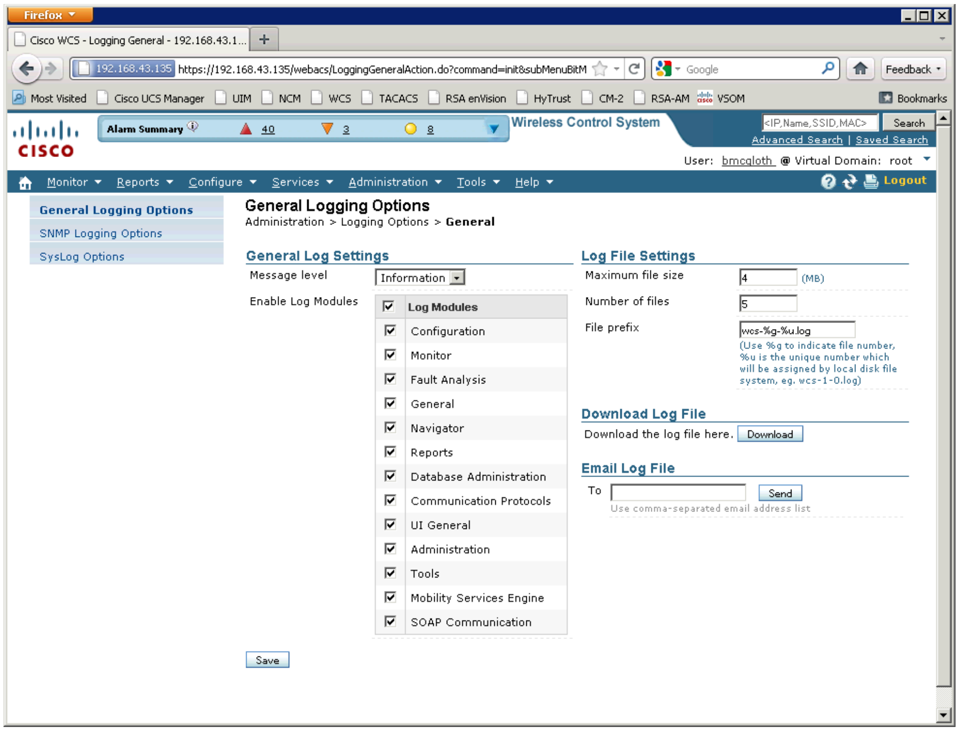
- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*

  Cisco Unified Wireless tracks individual administrator actions through several mechanisms including AAA, logging, and system events.

- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Figure 5-107 shows the configuration of local logging settings, and Figure 5-108 shows the syslog server configuration used to send logs to RSA enVision.

Figure 5-107 Local Logging Configuration



General Logging Options
Administration > Logging Options > **General**

General Log Settings

Message level: Information

Enable Log Modules:
- ☑ Log Modules
- ☑ Configuration
- ☑ Monitor
- ☑ Fault Analysis
- ☑ General
- ☑ Navigator
- ☑ Reports
- ☑ Database Administration
- ☑ Communication Protocols
- ☑ UI General
- ☑ Administration
- ☑ Tools
- ☑ Mobility Services Engine
- ☑ SOAP Communication

Save

Log File Settings

Maximum file size: 4 (MB)

Number of files: 5

File prefix: wcs-%g-%u.log
(Use %g to indicate file number, %u is the unique number which will be assigned by local disk file system, eg. wcs-1-0.log)

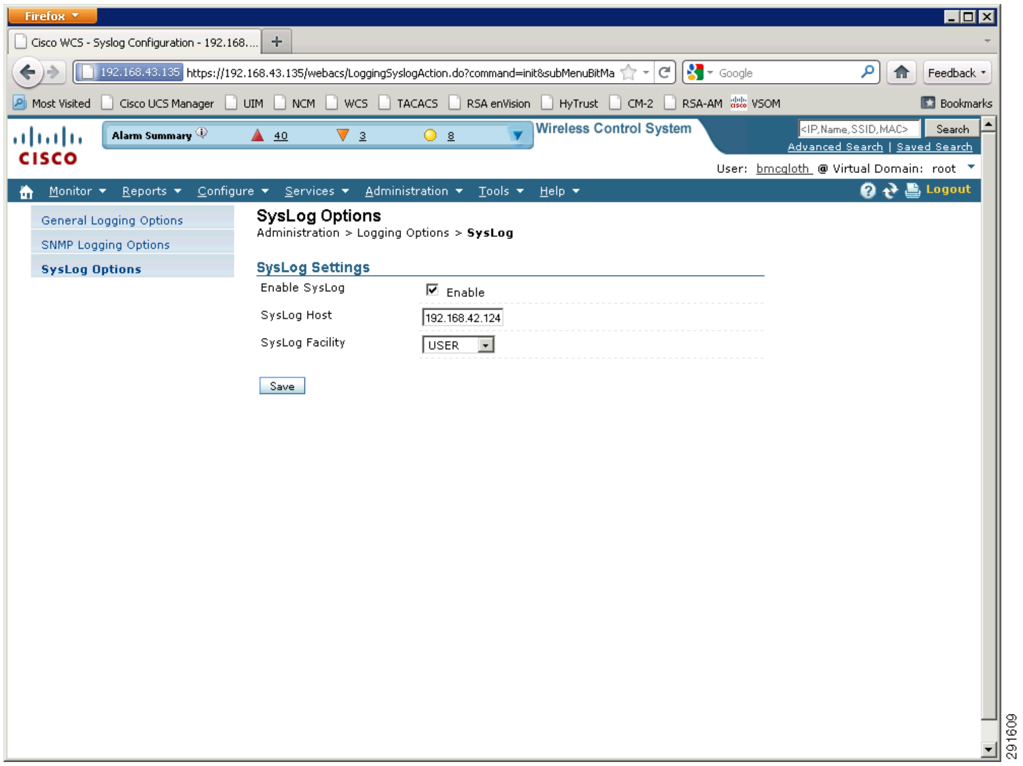
Download Log File

Download the log file here. Download

Email Log File

To: Send
Use comma-separated email address list

Figure 5-108 WCS Manager Syslog Configuration



SysLog Options

Administration > Logging Options > **SysLog**

SysLog Settings

Enable SysLog ☑ Enable

SysLog Host 192.168.42.124

SysLog Facility USER

Save

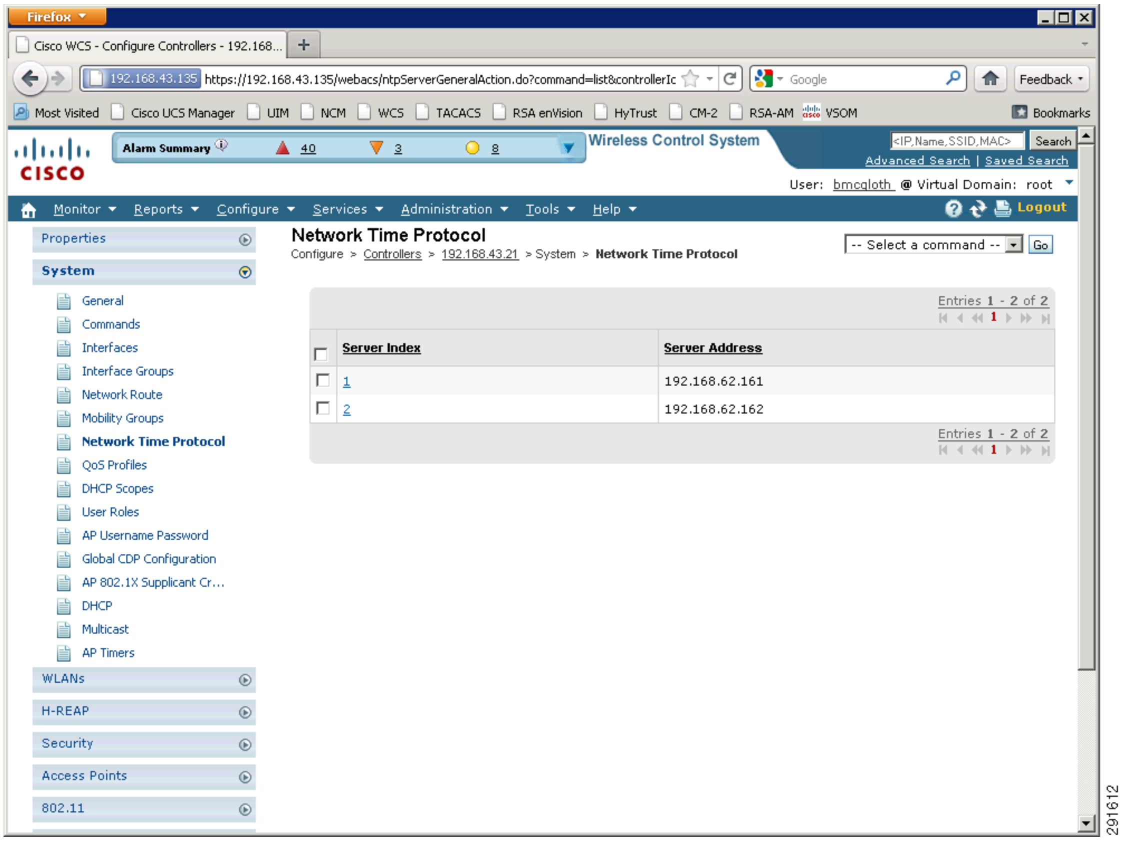
Cisco WCS uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

A Network Time Protocol server can be configured within the Cisco WCS and Controllers to meet this requirement for all wireless devices, as shown in Figure 5-109.

Figure 5-109 NTP Servers Screen for Controllers



Network Time Protocol

Configure > Controllers > 192.168.43.21 > System > Network Time Protocol

	Server Index	Server Address
□	1	192.168.62.161
□	2	192.168.62.162

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

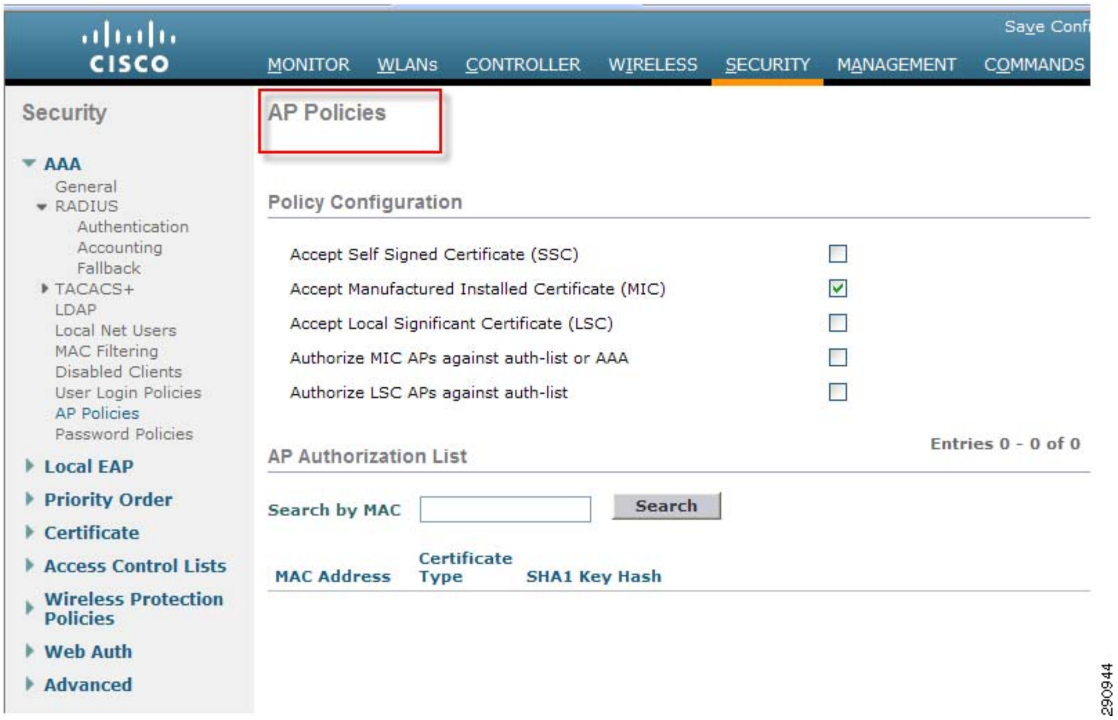
- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.1.b**—*Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:*
  - WLAN cards inserted into system components
  - Portable wireless devices connected to system components (for example, by USB, etc.)
  - Wireless devices attached to a network port or network device

  The Cisco WLAN performs 24-hour scanning to immediately detect and contain unauthorized and rogue wireless devices. Threats to network security can occur in between quarterly scans, creating the need to continuously scan and to use automatic alerts and containment mechanisms. Similarly, physical and/or port scanning on the wired network is not enough. Cisco Wireless LAN Controllers include wIPS and wIDS that find and stop rogue devices and attacks. WCS is a single point of management for WLAN devices, the mobility services engine, and mobility services. Cisco context-aware location services in the Cisco 3300 Series Mobility Services Engine (MSE) can locate multiple rogue devices. Cisco enhanced local mode (ELM) access points offer monitor mode wIPS on local mode access points for additional protection without a separate overlay network. Cisco CleanAir technology allows the detection and location of rogue devices on nonstandard Wi-Fi channels. (See Figure 5-110 and Figure 5-111.)

Figure 5-110 Security—AP Policies Screen



AP Policies

Policy Configuration

Accept Self Signed Certificate (SSC)	□
Accept Manufactured Installed Certificate (MIC)	☑
Accept Local Significant Certificate (LSC)	□
Authorize MIC APs against auth-list or AAA	□
Authorize LSC APs against auth-list	□

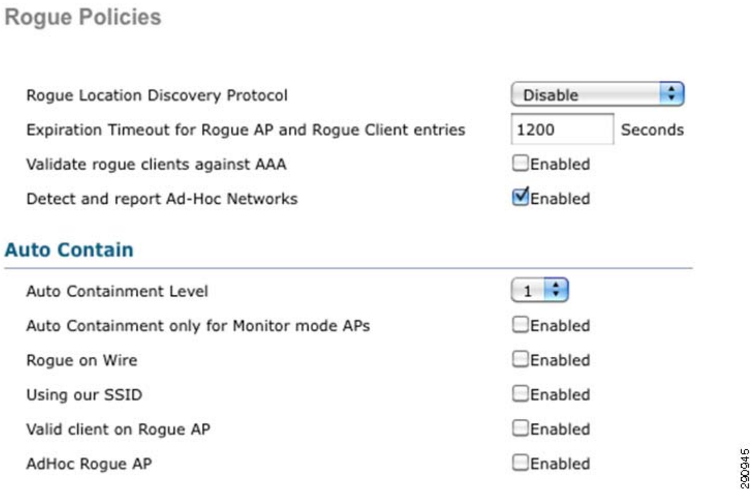
AP Authorization List

Entries 0 - 0 of 0

Search by MAC

MAC Address	Certificate Type	SHA1 Key Hash

Figure 5-111 Rogue Policies Screen



Rogue Policies

Rogue Location Discovery Protocol	Disable
Expiration Timeout for Rogue AP and Rogue Client entries	1200 Seconds
Validate rogue clients against AAA	□ Enabled
Detect and report Ad-Hoc Networks	☑ Enabled

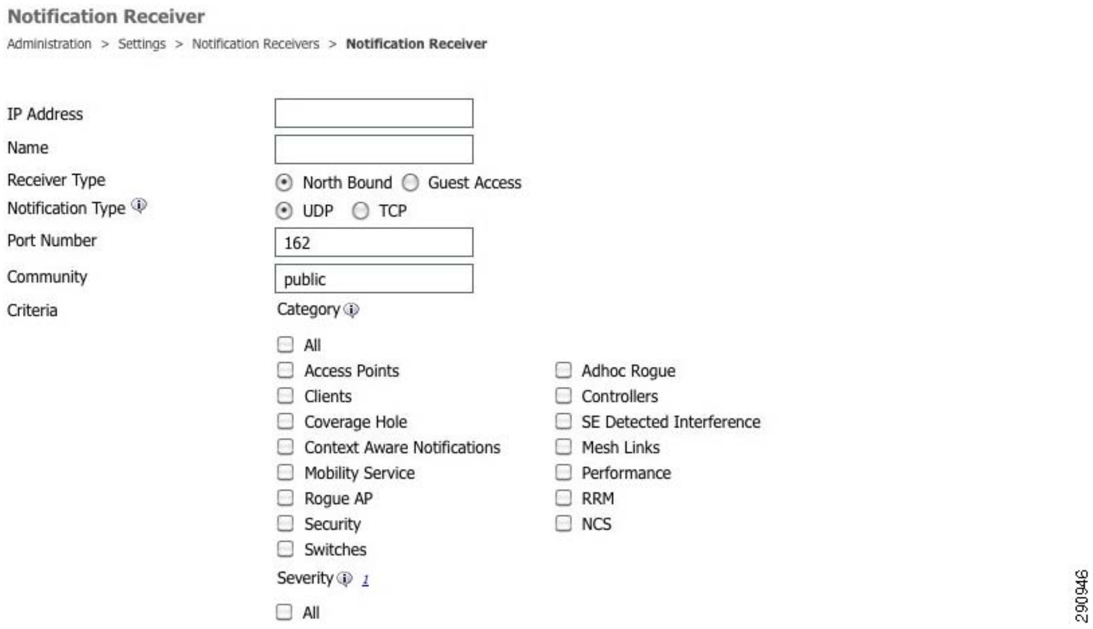
Auto Contain

Auto Containment Level	1
Auto Containment only for Monitor mode APs	□ Enabled
Rogue on Wire	□ Enabled
Using our SSID	□ Enabled
Valid client on Rogue AP	□ Enabled
AdHoc Rogue AP	□ Enabled

- **PCI 11.1.d**—*If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.*

Cisco WCS has the ability to forward alerts to e-mail addresses. The system can forward all or selected alerts to multiple receivers. (See Figure 5-112.)

Figure 5-112 Notification Receiver Screen



Notification Receiver

Administration > Settings > Notification Receivers > **Notification Receiver**

IP Address	
Name	
Receiver Type	● North Bound ○ Guest Access
Notification Type	● UDP ○ TCP
Port Number	162
Community	public
Criteria	Category

□ All	
□ Access Points	□ Adhoc Rogue
□ Clients	□ Controllers
□ Coverage Hole	□ SE Detected Interference
□ Context Aware Notifications	□ Mesh Links
□ Mobility Service	□ Performance
□ Rogue AP	□ RRM
□ Security	□ NCS
□ Switches	

Severity 1

□ All

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Storage

Cisco MDS Storage Switches

Cisco MDS storage switches provide the central switching infrastructure connecting servers to storage. They provide the added capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.

The Cisco MDS 9000 Series Multilayer SAN Switches can help lower the total cost of ownership of the most demanding storage environments. By combining robust and flexible hardware architecture with multiple layers of network and storage management intelligence, the Cisco MDS 9000 Series helps you build highly available, scalable storage networks with advanced security and unified management.

Table 5-51 PCI Assessment Summary—Cisco MDS Storage Switches

Models Assessed	
MDS 9506 (“Supervisor/Fabric-2”) version m9500-sf2ek9-mzg.5.0.1a.bin.S4 MDS 9506 (“Supervisor/Fabric-2”) version m9500-sf2ek9-mz.5.0.4.bin	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 3	3.4.1, 3.5, 3.5.1, 3.5.2, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of Cisco MDS storage switches is to securely encrypt cardholder data at rest as it passes from server to storage. (3.4)

Table 5-51 lists the component assessment details for Cisco MDS storage switches.

Table 5-52 Component Capability Assessment—Cisco MDS Storage Switches

Cisco MDS Storage Switches	
PRIMARY FUNCTION	Requirement 3 (3.4)
Securely encrypt cardholder data at rest.	
CAPABILITY	ASSESSMENT
Secure Services	
Disabled any unnecessary services—*“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

The MDS 9500s were configured for zoning and LUN masking to secure the logical partitioning of disk used for storing cardholder data. Only host machines in the data center that require access to that logical disk partition were allowed access. Configuration of the VSANs, host UUIDs, and mappings was partially performed using EMC Unified Infrastructure Manager as directed by the Vblock architecture by VCE. Vblock requires specific software versions and pre-configurations to be completed as specified in the Vblock preparation guide.

More information of Vblock designs can be found at the following URL:
http://www.vceportal.com/solutions/68580567.html#

Information in installing and configuring Cisco MDS can be found at the following URL:
http://www.cisco.com/en/US/products/hw/ps4159/ps4358/tsd_products_support_series_home.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

The Cisco MDS 9000 NX-OS Software does not use defaults for system passwords and other security parameters, but instead prompts the user for this information at power-up and can enforce the use of PCI-compliant passwords.

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are two ways to do this: initial setup, or configuration after the fact.

  1. Initial setup

```
 ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
Do you want to enforce secure password standard (yes/no) [y]: yes
Create another login account (yes/no) [n]:
Configure read-only SNMP community string (yes/no) [n]: yes
Configure read-write SNMP community string (yes/no) [n]: yes
Enter the switch name :
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
Mgmt0 IPv4 address :
Configure the default gateway? (yes/no) [y]:
IPv4 address of the default gateway :
Configure advanced IP options? (yes/no) [n]:
Enable the ssh service? (yes/no) [y]: yes
Type of ssh key you would like to generate (dsa/rsa) [rsa]:
Number of rsa key bits <768-2048> [1024]:
Enable the telnet service? (yes/no) [n]: no
Enable the http-server? (yes/no) [y]: no
Configure clock? (yes/no) [n]:
Configure timezone? (yes/no) [n]:
Configure summertime? (yes/no) [n]:
Configure the ntp server? (yes/no) [n]: yes
Configure default switchport interface state (shut/noshut) [shut]: shut
Configure default switchport trunk mode (on/off/auto) [on]:
Configure default switchport port mode F (yes/no) [n]: yes
Configure default zone policy (permit/deny) [deny]: deny
Enable full zoneset distribution? (yes/no) [n]:
Configure default zone mode (basic/enhanced) [basic]:
```

  2. By configuration after the fact

```
Configure terminal
Password strength-check
snmp-server community <password> ro
snmp-server community <password> rw
feature ssh
ssh key dsa or ssh key rsa <768-2048>
no feature telnet
no feature http-server
ntp server <ip address>
system default switchport shutdown
system default switchport mode f
no system default zone default-zone permit
```

  3. Additional

```
Secure access to management port:
ip access-list 23 permit ip 127.0.0.1 0.0.0.0 <mgmt port ip address> 0.0.0.0
ip access-list 23 permit ip <ip address of mgmt workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 permit ip <ip address of snmp workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 permit ip <ip address of AAA server> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 permit ip <ip address of NTP workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 deny ip any any log-deny
interface mgmt0
ip address <ip address> <mask>
ip access-group 23 in
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco MDS switch is a hardened device that does not allow changes to the operating system.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The Cisco MDS switch uses SSL for web-based administrative and user access, and uses SSH for remote terminal access by implementing the configurations shown above.

Requirement 3: Protect Stored Cardholder Data

Cisco Storage Media Encryption (SME) provides protection of cardholder data by delivering disk and tape encryption. Cisco SME stores the keys in the Cisco key management server or in a secure third-party key manager such as RSA KM.

- **PCI 3.4.1**—*If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.*

  Although the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these switches provide the capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.

  The SME feature of the Cisco MDS 9000 SAN fabric is independent of the native operating system access control. Decryption keys are managed by the Cisco Key Manager, which is part of the SME feature. Keys are tied to individual tapes or LUNs, not to user accounts.

- **PCI 3.5**—*Protect any keys used to secure cardholder data against disclosure and misuse. Note: This requirement also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*

  All keys are stored in encrypted form, and are always encrypted for transmission within the fabric.

- **PCI 3.5.1**—*Restrict access to cryptographic keys to the fewest number of custodians necessary.*

  Only recovery officers have access to the master key, stored in the PIN-protected smart cards. Only the key administrators have access to the disk and tape keys, stored in encrypted format in the Cisco Key Manager Center (KMC) or the RSA key manager.

- **PCI 3.5.2**—*Store cryptographic keys securely in the fewest possible locations and forms.*

Keys are stored in encrypted form in Cisco Key Manager, or stored by Cisco Key Manager in the RSA Key Manager. Both key managers provide for secure backup and recovery of keys, and for their secure storage in an alternate location. The master key is spread across multiple smart cards, each protected by a PIN chosen by the depository recovery officer.

- **PCI 3.6.1**—*Generation of strong cryptographic keys*

  The cryptographic keys (AES 256 bits) are generated by the encryption engine within the services node.

- **PCI 3.6.2**—*Secure cryptographic key distribution*

  The keys are never transmitted in clear text, but always using secure protocols (HTTPS and SSL).

- **PCI 3.6.3**—*Secure cryptographic key storage*

  Key-encrypting keys are stored in encrypted format in the Cisco KMC. Master keys are stored in PIN-encrypted format in the smart cards.

- **PCI 3.6.4**—*Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of ciphertext has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).*

  Cisco SME offers the capability to re-key and change keys as needed. Customers must enforce and document this procedure appropriately.

- **PCI 3.6.5**—*Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*

  Cisco KMC can manage the complete key lifecycle. Customers need to implement and document this procedure appropriately.

Requirement 6: Develop and Maintain Secure Systems and Applications

Cisco MDS 9000 NX-OS provides the capability to use a test VSAN to validate any new configuration before production. Cisco MDS 9000 NX-OS has also been developed with secure coding guidelines and is tested against common vulnerabilities.

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco MDS switches. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

Cisco MDS 9000 Family security features such as VSANs, advanced zoning, fabric binding, port security, Fibre Channel Security Protocol (FC-SP) authentication, and role-based access control (RBAC) with SNMPv3 and SSH make the Cisco MDS 9000 Family an excellent platform for enforcing this requirement. SSH RBAC in particular, if used in conjunction with VSANs, is especially designed to support tight partitioning of the physical infrastructure.

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS using TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- This is accomplished using the user role feature (see 7.2.2).
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- This is accomplished using the user role feature (see 7.2.2).
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

The following configurations demonstrate how to configure the Cisco MDS for TACACS+ authentication to a central server.

```
Feature tacacs+

tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131

aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable
```

Note To configure LDAP authentication in NX-OS version 5.0 or higher, enable LDAP (**feature ldap**) and follow configuration steps in the Cisco MDS 9000 Family NX-OS Security Configuration Guide.

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*

```
Feature privilege
    change admin user ID:
    username admin password <password> role network-admin (password will be
encrypted when displayed)
    create network operator type user ID:
    username <assigned name> password <password> role network-operator (password
will be encrypted when displayed)
    create default user ID:
    role name default-role
        description This is a system defined role and applies to all users.
        rule 5 permit show feature environment
        rule 4 permit show feature hardware
        rule 3 permit show feature module
        rule 2 permit show feature snmp
        rule 1 permit show feature system
    username <assigned name> password <password> role default-role (password will
be encrypted when displayed)
    create custom user ID:
    role name <name>
        description User defined permissions define here:
        rule 1 permit show interface
        .
        .
        Rune 256 permit show module
    username <assigned name> password <password> role <name> (password will be
encrypted when displayed)
```

- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  All user access is controlled by the user role function; there is no generic user access.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

The Cisco MDS 9000 Family provides the capability to create an individual account for each administrator with a strong password. Authentication can be performed using the external authentication, authorization, and accounting (AAA) server of choice (for example, TACACS+) to implement the desired user authentication and password management policies.

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  To enforce session lengths, enable this using **terminal session-timeout** <*time in minutes*>.

  ```
  line vty
    exec-timeout 15
  line console
    exec-timeout 15
  ```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco MDS 9000 Family implements the Cisco Data Center Network Manager (DCNM), which continuously monitors the SAN and allows you to establish criteria and thresholds to generate real-time alarms and call-home functions. Syslog offers detailed entries and can be redirected to a log server to consolidate IT infrastructure monitoring information. Note that the log never contains application data.

Cisco MDS is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6—***Identity or name of affected data, system component, or resource.*

Cisco MDS uses the local clock facilities to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco MDS use NTP to meet these requirements by implementing the following configuration statements:

  ```
  clock timezone PST -8 0
  clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
  ntp server 192.168.62.161
  ```

```
ntp server 192.168.62.162
```

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco MDS is capable of sending system events to a centralized repository using the syslog function and SNMP traps. Logs stored locally are buffered and require operator level privileges on the router to be viewed. External logging and SNMP traps are enabled by implementing the following configuration statements:

  ```
  logging server 192.168.42.124 6
  ```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Security

Cisco ASA 5500 Series—Store

The Cisco ASA 5500 Series Adaptive Security Appliances provide secure segmentation within the store. Their stateful firewall and modular intrusion detection modules enable the store to securely connect public networks to the cardholder data environment.

The Cisco ASA 5500 Series delivers superior scalability, a broad span of technology and solutions, and effective, always-on security designed to meet the needs of a wide array of deployments. By integrating the world's most proven firewall; a comprehensive, highly effective intrusion prevention system (IPS) with Cisco Global Correlation and guaranteed coverage; high-performance VPN and always-on remote access, the Cisco ASA 5500 Series helps organizations provide secure, high performance connectivity and protects critical assets for maximum productivity.

The Cisco ASA 5500 Series includes the Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580, and 5585-X Adaptive Security Appliances-purpose-built, high-performance security solutions that take advantage of Cisco expertise in developing industry-leading, award-winning security and VPN solutions. Through Cisco Multi-Processor Forwarding (MPF), the Cisco ASA 5500 Series brings a new level of security and policy control to applications and networks. MPF enables highly customizable, flow-specific security policies that have been tailored to application requirements. The performance and extensibility of the Cisco ASA 5500 Series is enhanced through user-installable security service modules (SSMs). This adaptable architecture enables businesses to rapidly deploy security services when and where they are needed, such as tailoring inspection techniques to specific application and user needs or adding additional intrusion prevention and content security services such as those delivered by the Adaptive Inspection and Prevention (AIP) and Content Security and Control (CSC) SSMs. Furthermore, the modular hardware architecture of the Cisco ASA 5500 Series, along with the powerful MPF, provides the flexibility to meet future network and security requirements, extending the outstanding investment protection provided by the Cisco ASA 5500 Series and allowing businesses to adapt their network defenses to new threats as they arise.

All Cisco ASA 5500 Series appliances offer both IPsec and SSL/DTLS VPN solutions; clientless and AnyConnect VPN features are licensed at various price points, on a per-seat and per-feature basis. By converging SSL and IPsec VPN services with comprehensive threat defense technologies, the Cisco ASA 5500 Series provides highly customizable, granular network access tailored to meet the requirements of diverse deployment environments, while providing advanced endpoint and network-level security.

Table 5-53 PCI Assessment Summary—Cisco ASA 5500 Series (Store)

Models Assessed	
Cisco ASA5510 w/SSM-10 version asa841-k8.bin and IDS version 7.0(4)	
PCI Sub-Requirements Passed	
PCI 1	1.2.1, 1.2.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 4	4.1
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI 11	11.4
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The main function of the store Cisco ASA firewall is to securely segment public and cardholder data environment store networks, and provide intrusion detection capabilities. (1.2, 1.3, 11.4)

Table 5-53 lists the component assessment details for the Cisco ASA 5500 Series.

Table 5-54 Component Capability Assessment—Cisco ASA 5500 Series (Store)

Cisco ASA 5500 Series (Store)	
PRIMARY FUNCTION	Requirement 1, 11 (1.2, 1.3, 11.4)
Segment public and cardholder data environment networks within the store.	
CAPABILITY	ASSESSMENT
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- Select the appropriate Cisco ASA model and SSM module for the traffic needs in the store.
- Connect the SSM module to the secure management segment of the store network using the external Ethernet interface.
- Configure security policies, objects, and rules centrally with Cisco Security Manager.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco ASA firewalls are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted.

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Firewall configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of firewalls, routers, and switches are synchronized. Additionally, Cisco Security Manager stores a copy of the firewall configuration for the policies that it manages.

- **PCI 1.2.3**—*Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.*
- **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*
- **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

The following configuration example shows how objects identify hosts and services within the network and their use in an access list to permit approved traffic:

```
!
interface Ethernet0/0
 nameif MSP-WAN
 security-level 0
 ip address 10.10.255.176 255.255.255.0
!
interface Ethernet0/1.1000
 vlan 1000
 nameif MANAGEMENT
 security-level 100
 ip address 10.10.191.1 255.255.255.0
!
! ----Defining Objects and Object Groups----
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 network-object 192.168.42.122 255.255.255.255
object-group network CSManager
 description Cisco Security Manager
 network-object 192.168.42.133 255.255.255.255
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 network-object 192.168.42.124 255.255.255.255
object-group network AdminStation3
 network-object 192.168.42.138 255.255.255.255
object-group network POS-Store-MSP
 network-object 10.10.176.81 255.255.255.255
!
object-group service CSM_INLINE_svc_rule_73014461184
 description Generated by CS-Manager from service of FirewallRule# 4
(ASA-Store_V2/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object object ORACLE-OAS
 service-object object TOMAX-8990
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object HTTPS-8443
!
object-group network CSM_INLINE_src_rule_73014461184
 description Generated by CS-Manager from src of FirewallRule# 4
(ASA-Store_V2/mandatory)
 group-object DC-POS-Tomax
 network-object object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
! ----One line of the larger access-list permitting traffic----
!
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461184
object-group CSM_INLINE_src_rule_73014461184 object-group POS-Store-MSP
!
! ----Applying the access-list to an interface----
!
access-group OUTSIDE in interface MSP-WAN
```

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco ASA firewalls allow only administrative connections from authorized hosts/networks, as specified in the device configuration. The HTTP server supports only secure connections using SSL. If no hosts or networks are specified for the service, it is effectively disabled (for example, the Telnet service). The following configuration shows the authorized management hosts for SSH and HTTPS administration, and none for Telnet.

```
http server enable
http 10.19.151.99 255.255.255.255 north
http 192.168.41.101 255.255.255.255 south
http 192.168.41.102 255.255.255.255 south
http 192.168.42.122 255.255.255.255 south
http 192.168.42.124 255.255.255.255 south
http 192.168.42.133 255.255.255.255 south
http 192.168.42.138 255.255.255.255 south
telnet timeout 5
ssh 10.19.151.99 255.255.255.255 north
ssh 192.168.41.101 255.255.255.255 south
ssh 192.168.41.102 255.255.255.255 south
ssh 192.168.42.122 255.255.255.255 south
ssh 192.168.42.124 255.255.255.255 south
ssh 192.168.42.133 255.255.255.255 south
ssh 192.168.42.138 255.255.255.255 south
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco ASA firewalls do not have any unnecessary services enabled by default.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

Cisco ASA firewalls support strong encryption for SSH and HTTPS. The following configurations are used to configure strong cryptography:

```
! ---Specify only Strong algorithms for SSL connections---
!
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1
!
! ---Specify strong encryption version of SSH
!
ssh version 2
!
```

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco ASA Firewalls. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS using TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel’s job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*

- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco ASAs are configured to use a AAA model for user-based access. Users can be assigned to groups and, based on privilege levels, have access to only the information they require for their job function. By default in Cisco ASA, no users are allowed access unless specifically configured and assigned appropriate passwords.

```
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (MANAGEMENT) host 192.168.42.131
 key <removed>
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
```

  Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

  These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa authentication ssh console RETAIL LOCAL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

The Cisco ASA is able to meet some of the requirements locally, as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco ASA supports the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco ASA require setting of a password.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of strong MD5-encrypted hashing of locally stored passwords, Cisco ASA also supports the use of AES encryption of pre-shared keys.

```
password encryption aes
```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco ASAs do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Security Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco ASA does not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Security Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco ASA does not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco ASA does not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco ASA does not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

  PCI 8.5.13—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco ASA management interfaces are configured as follows to meet this requirement:

  ```
  http server idle-timeout 15
  ssh timeout 15
  ```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco ASA 5500 is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*

- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*

  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*

  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco ASA uses the local clock facilities meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco ASA use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.162 source MSP-WAN
ntp server 192.168.62.161 source MSP-WAN prefer
clock timezone PST -8
clock summer-time PDT recurring
```

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco ASA is capable of sending system events to a centralized repository using the syslog function and SNMP traps. Logs stored locally are buffered and require operator level privileges on the router to be viewed. External logging and SNMP traps are enabled by implementing the following configuration statements:

```
logging enable
logging trap debugging
logging asdm debugging
logging host MSP-WAN 192.168.42.124
```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco ASA 5500 Series—Data Center

As a core component of Cisco Borderless Networks, Cisco ASA 5500 Series Adaptive Security Appliances provide:

- Context-aware firewall capabilities
- Proven firewall services
- Comprehensive real-time threat defense
- Effective, always-on, highly secure remote access
- Highly secure communication services

These solutions help reduce deployment and operational costs while delivering comprehensive network security for networks of all sizes.

Context-aware firewalling capabilities combine:

- In-depth local network context from TrustSec
- Real-time global threat intelligence from Cisco Security Intelligence Operations (SIO)
- Unique mobile client insight from AnyConnect

In addition, these solutions offer an advanced intrusion prevention system (IPS) with Global Correlation, which is twice as effective as a traditional IPS and includes Cisco guaranteed coverage.

Table 5-55 PCI Assessment Summary—Cisco ASA 5500 Series (Data Center)

Models Assessed	
ASA5540 w/SSM-40 asa841-k8.bin ASA5540 w/SSM-20 asa841-k8.bin ASA5585-S60-2A-K9 asa824-smp-k8.bin	
PCI Sub-Requirements Passed	
PCI 1	1.2.1, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 4	4.1
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.3, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI 11	11.4
PCI Sub-Requirements Requiring Compensating Controls	

Table 5-55 PCI Assessment Summary—Cisco ASA 5500 Series (Data Center) (continued)

No compensating controls were required to satisfy any sub-requirements.
PCI Sub-Requirements Failed
No sub-requirements were failed.

Primary PCI Function

The primary functions of the data center firewalls are twofold. They operate as a firewall, restricting traffic between the cardholder data environment and other areas of the network; and they operate as an intrusion prevention system, inspecting all traffic going to and from the cardholder data environment. These controls map directly to satisfying a number of PCI sub-requirements including Requirements 1, 2, 4, 7, 8, 10, and 11. The following is a description of how each of the PCI sub-requirements is satisfied for store routers.

Table 5-55 lists the component assessment details for Cisco ASA 5500 Series.

Table 5-56 Component Capability Assessment —Cisco ASA 5500 Series (Data Center)

Cisco ASA 5500 Series (Data Center)	
PRIMARY FUNCTION	**Requirement 1, 11 (1.2, 1.3, 11.4)**
Restrict traffic between the cardholder data environment and other network areas, and as an IPS.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- Implementing Cisco ASA firewalls in transparent mode helps reduce network complexity.

- IDS/IPS modules require the external network interface port to be connected to the network for management and automated reporting and alerts to be sent.
- When configuring high availability, only the primary Cisco ASA needs to be fully configured; the secondary Cisco ASA mirrors the primary's configurations once the failover interface and IP information are configured.
- Cisco Adaptive Security Device Manager (ADSM) is a good tool for making policy changes in small environments. For large enterprises, Cisco Security Manager provides the best platform for managing rules with a large number of objects across many devices.
- Multi-context firewalls allow for traffic and administrative segmentation.
- Firewall rule sets must adhere to a "least amount of access necessary" policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment (for example, point-of-sale) networks.
- Configure the primary login authentication of the Cisco ASA to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the Cisco ASA itself in the event of a WAN or Cisco Secure ACS failure.
- Configure logs to be sent to a centralized syslog server such as RSA enVision.
- Configure NTP to ensure all logging is coordinated
- Cisco ASA firewalls were used for the store WAN, Internet edge, and data center aggregation block.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco ASA firewalls are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted.
- **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*
- **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

  The following configuration example shows how objects identify hosts and services within the network and their use in an access list to permit approved traffic:

```
!
! ----Naming of interfaces as assigned from the Admin Context----
!
```

```
interface outside
 nameif north
 bridge-group 1
 security-level 0
!
interface inside
 nameif south
 bridge-group 1
 security-level 100
!
! ----Defining Objects and Object Groups----
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 network-object 192.168.42.122 255.255.255.255
object-group network CSManager
 description Cisco Security Manager
 network-object 192.168.42.133 255.255.255.255
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 network-object 192.168.42.124 255.255.255.255
object-group network AdminStation3
 network-object 192.168.42.138 255.255.255.255
object-group network Admin-Systems
 group-object EMC-NCM
 group-object AdminStation
 group-object AdminStation2
 group-object CSManager
 group-object RSA-enVision
 group-object AdminStation3
 group-object AdminStation4-bart
!
object-group service CSM_INLINE_svc_rule_77309411635
 description Generated by CS-Manager from service of FirewallRule# 3
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq ssh
 service-object tcp destination eq https
 group-object HTTPS-8443
!
object-group network CSM_INLINE_dst_rule_77309411635
 description Generated by CS-Manager from dst of FirewallRule# 3
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
 group-object DC-DMZ
!
! ----One line of the larger access-list permitting traffic----
!
access-list CSM_FW_ACL_south extended permit object-group
CSM_INLINE_svc_rule_77309411635 object-group Admin-Systems object-group
CSM_INLINE_dst_rule_77309411635
!
! ----Applying the access-list to an interface----
!
access-group CSM_FW_ACL_south in interface south
```

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco ASA firewalls allow only administrative connections from authorized hosts/networks, as specified in the device configuration. The HTTP server supports only secure connections using SSL. If no hosts or networks are specified for the service, it is effectively disabled (for example, the Telnet service). The following configuration shows the authorized management hosts for SSH and HTTPS administration, and none for Telnet.

```
http server enable
http 10.19.151.99 255.255.255.255 north
http 192.168.41.101 255.255.255.255 south
http 192.168.41.102 255.255.255.255 south
http 192.168.42.122 255.255.255.255 south
http 192.168.42.124 255.255.255.255 south
http 192.168.42.133 255.255.255.255 south
http 192.168.42.138 255.255.255.255 south
telnet timeout 5
ssh 10.19.151.99 255.255.255.255 north
ssh 192.168.41.101 255.255.255.255 south
ssh 192.168.41.102 255.255.255.255 south
ssh 192.168.42.122 255.255.255.255 south
ssh 192.168.42.124 255.255.255.255 south
ssh 192.168.42.133 255.255.255.255 south
ssh 192.168.42.138 255.255.255.255 south
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco ASA firewalls do not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco ASA firewalls support strong encryption for SSH and HTTPS. The following configurations are used to configure strong cryptography:

```
! ---Specify only Strong algorithms for SSL connections---
!
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1
!
! ---Specify strong encryption version of SSH
!
ssh version 2
!
```

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

Requirement 6: Develop and Maintain Secure Systems and Applications

PCI 6.1—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco ASA firewalls. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

To meet all of the requirements listed below, the PCI solution for retail uses a centralized user database in the Active Directory, which is linked via LDAP, RADIUS, and TACACS+ services. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. This resource is used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco ASA firewalls are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco ASA firewalls, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (south) host 192.168.42.131
 key *****
aaa authentication ssh console RETAIL LOCAL
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa accounting ssh console RETAIL
aaa accounting enable console RETAIL
aaa accounting command privilege 15 RETAIL
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
```

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication ssh console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco firewalls to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure Access Control Server must be implemented. Configure AAA services as shown above in requirement 7.

The firewall is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco firewalls support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username csmadmin password <removed> encrypted privilege 15
  username retail password <removed> encrypted privilege 15
  username bmcgloth password <removed> encrypted privilege 15
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  When configuring local user accounts, you must specify a password to achieve PCI compliance. Do not use the “nopassword” option.

  ```
  username csmadmin password <removed> encrypted privilege 15
  username retail password <removed> encrypted privilege 15
  username bmcgloth password <removed> encrypted privilege 15
  ```

- **PCI 8.3**—*Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) Note: Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.*

  Using AAA services, Cisco ASA firewalls can support two-factor authentication by pointing to an external authentication server (as described in Requirement 7). In the test environment, a second authentication service was set up using RSA Access Manager and SecurID tokens for generating one-time passwords. The following configurations show the setup of the additional AAA RADIUS server and authentication group for SSL VPN access from external sources.

```
aaa-server partnerauth protocol radius
aaa-server partnerauth (inside) host 192.168.42.137
 timeout 5
 key *****
 radius-common-pw *****

webvpn
 enable outside
 internal-password enable
 smart-tunnel list AllExternalApplications All-Applications * platform windows
group-policy DfltGrpPolicy attributes
 webvpn
  url-list value page1
  smart-tunnel enable AllExternalApplications
group-policy Retail-PCI internal
group-policy Retail-PCI attributes
 vpn-tunnel-protocol ssl-clientless
!
tunnel-group DefaultRAGroup general-attributes
 authentication-server-group partnerauth
tunnel-group DefaultWEBVPNGroup general-attributes
 authentication-server-group partnerauth
tunnel-group Retail-Lab type remote-access
tunnel-group Retail-Lab general-attributes
 authentication-server-group partnerauth LOCAL
 default-group-policy Retail-PCI
```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  All local passwords on the firewall are stored using strong encryption. Additionally, the following command can be used to encrypt local keys:

  ```
  key config-key password-encryption
  password encryption aes
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco ASA firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager or Cisco Security Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco ASA firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager or Cisco Security Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco ASA firewalls do not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco ASA firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

Cisco ASA firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco ASA firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco ASA firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco ASA firewalls are able to time-out administrative sessions using the following configuration statements:

  ```
  !
  http server idle-timeout 15
  !
  ssh timeout 15
  !
  console timeout 15
  ```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco ASA firewalls are able to track and monitor all administrative user access, events such as interface up/down, dropped or filtered traffic, device authentications, and VPN sessions, to name a few.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco ASA firewalls track individual administrator actions as identified in the requirements above (10.1, 10.2 and 10.3) through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging enable
logging trap debugging
logging asdm debugging
logging host inside 192.168.42.124
```

Cisco ASA firewalls use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco ASA firewalls use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.162 source inside
ntp server 192.168.62.161 source inside prefer

clock timezone PST -8
clock summer-time PDT recurring
```

To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Note The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco Firewall Services Module (FWSM)—Data Center

The Cisco Firewall Services Module (FWSM) is an integrated module installed inside a Cisco Catalyst 6500 Series Switch or Cisco 7600 Internet Router. The Cisco FWSM allows any port on the Cisco Catalyst switch to operate as a firewall port and integrates firewall security inside the network infrastructure.

The Cisco FWSM includes a number of advanced features that help reduce costs and operational complexity while enabling organizations to manage multiple firewalls from the same management platform. Features such as the resource manager help organizations limit the resources allocated to any security context at any time, thus ensuring that one security context does not interfere with another. The transparent firewall feature configures the Cisco FWSM to act as a Layer 2 bridging firewall, resulting in minimal changes to network topology.

Table 5-57 PCI Assessment Summary—Cisco FWSM

Models Assessed	
WS-SVC-FWM version c6svc-fwm-k9.4-1-5.bin	
PCI Sub-Requirements Passed	
PCI 1	1.2.1, 1.2.2, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 4	4.1
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary function of the Cisco FWSM is to restrict traffic between the cardholder data environment and other areas of the network (1.2, 1.3).

Table 5-57 lists the component assessment details for the Cisco FWSM.

Table 5-58 Component Capability Assessment—Cisco FWSM

Cisco FWSM	
PRIMARY FUNCTION	**Requirement 1 (1.2, 1.3)**
Restrict traffic between the cardholder data environment and other network areas.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- Firewall rule sets must adhere to a "least amount of access necessary" policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports.
- For Internet edge, disable **icmp permit** on the outside interface of Cisco FWSM. If users need to access servers in the DMZ segment, make sure that external users can reach the servers using very specific protocol and ports.
- Configure the **ip verify reverse path** command on all interfaces to provide anti-spoofing functionality.
- Configure the console timeout commands to 15 minutes or less on the console of the Cisco FWSM.
- Configure appropriate banner messages on login, incoming, and exec modes of the Cisco FWSM. The login banner warning should not reveal the identity of the company that owns or manages the Cisco FWSM. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the Cisco FWSM to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the Cisco FWSM itself in the event of connectivity or Cisco Secure ACS failure.
- Change default passwords and community strings to appropriate complexity.

- Allow only SSHv2 (and not Telnet or SSHv1) connection from network management station to Cisco FWSM.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco FWSM firewalls are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted.

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Firewall configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of firewalls, routers, and switches are synchronized. Additionally, Cisco Security Manager stores a copy of the firewall configuration for the policies that it manages.

- **PCI 1.3**—*Prohibit direct public access between the Internet and any system component in the cardholder data environment.*

  Cisco FWSM firewalls track and monitor the state of communications and are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted. FWSM firewalls have multiple interfaces and VLAN support, allowing for segmentation of traffic and the creation of DMZ zones or areas with differing security policies. Cisco ASA firewalls can also perform NAT to aid in securing/obscuring the private IP addressing information used within an enterprise.

  - **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
  - **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
  - **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
  - **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
  - **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
  - **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
  - **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*
  - **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

  The following configuration example shows how objects identify hosts and services within the network and their use in an access list to permit approved traffic:

```
!
! ----VLAN's assigned from the Host Catalyst Switch----
!
interface Vlan21
 nameif inside
 security-level 100
 ip address 192.168.21.10 255.255.255.0
!
```

```
interface Vlan22
 nameif outside
 security-level 0
 ip address 192.168.22.1 255.255.255.0 standby 192.168.22.2
!!
! ----Defining Objects and Object Groups----
!
object-group network DC-ALL
 description All of the Data Center
 network-object 192.168.0.0 255.255.0.0
object-group network Stores-ALL
 description all store networks
 network-object 10.10.0.0 255.255.0.0
!
object-group service CSM_INLINE_svc_rule_81604379580 tcp
 description Generated by CS-Manager from service of FirewallRule# 7
(FWSM-DMZ-1_v1/mandatory)
 port-object eq smtp
 port-object eq https
 port-object eq ssh
!
object-group network CSM_INLINE_src_rule_81604379580
 description Generated by CS-Manager from src of FirewallRule# 7
(FWSM-DMZ-1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
! ----One line of the larger access-list permitting traffic----
!
access-list INSIDE extended permit tcp object-group CSM_INLINE_src_rule_81604379580
192.168.23.64 255.255.255.224 object-group CSM_INLINE_svc_rule_81604379580
!
! ----Applying the access-list to an interface----
!
access-group INSIDE in interface inside
```

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco FWSM firewalls allow only administrative connections from authorized hosts/networks, as specified in the device configuration. The HTTP server supports only secure connections using SSL. If no hosts or networks are specified for the service, it is effectively disabled (for example, the Telnet service). The following configuration shows the authorized management hosts for SSH and HTTPS administration, and none for Telnet.

```
http server enable
http 10.19.151.99 255.255.255.255 north
http 192.168.41.101 255.255.255.255 south
http 192.168.41.102 255.255.255.255 south
http 192.168.42.122 255.255.255.255 south
http 192.168.42.124 255.255.255.255 south
http 192.168.42.133 255.255.255.255 south
http 192.168.42.138 255.255.255.255 south

ssh 10.19.151.99 255.255.255.255 north
ssh 192.168.41.101 255.255.255.255 south
ssh 192.168.41.102 255.255.255.255 south
ssh 192.168.42.122 255.255.255.255 south
ssh 192.168.42.124 255.255.255.255 south
ssh 192.168.42.133 255.255.255.255 south
ssh 192.168.42.138 255.255.255.255 south
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco FWSM firewalls do not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco FWSM firewalls support strong encryption for SSH and HTTPS. The following configurations are used to configure strong cryptography:

```
!
! ---Specify strong encryption version of SSH
!
ssh version 2
!
```

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco FWSM modules. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*

- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco FWSM firewalls are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco FWSM firewalls, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (south) host 192.168.42.131
 key <removed>
aaa authentication ssh console RETAIL LOCAL
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa accounting ssh console RETAIL
aaa accounting enable console RETAIL
aaa accounting command privilege 15 RETAIL
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
```

  Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

  These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication ssh console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco firewalls to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure Access Control Server must be implemented. Configure AAA services as shown above in requirement 7.

The firewall is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco firewalls support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  When configuring local user accounts, you must specify a password to achieve PCI compliance. Do not use the "nopassword" option.

  ```
  username csmadmin password <removed> encrypted privilege 15
  username retail password <removed> encrypted privilege 15
  username bmcgloth password <removed> encrypted privilege 15
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  All local passwords on the firewall are stored using strong encryption. Additionally, the following command can be used to encrypt local keys:

  ```
  password encryption aes
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco FWSM firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager or Cisco Security Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco FWSM firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager or Cisco Security Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco FWSM firewalls do not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco FWSM firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco FWSM firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco FWSM firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco FWSM firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco FWSM firewalls are able to time-out administrative sessions using the following configuration statements:

  ```
  !
  http server idle-timeout 15
  !
  ssh timeout 15
  !
  console timeout 15
  ```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco FWSM firewalls are able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco FWSM firewalls use the local clock facilities of the host Cisco Catalyst chassis to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Cisco Virtual Security Gateway

The Cisco Virtual Security Gateway (VSG) for Cisco Nexus 1000V Series Switches was used in the data center for setting a boundary between the sensitive scope of the retailer's cardholder data environment and out-of-scope networks. It is a virtual firewall for Cisco Nexus 1000V Series Switches that delivers security and compliance for virtual computing environments. Cisco VSG uses virtual service data path (vPath) technology embedded in the Cisco Nexus 1000V Series Virtual Ethernet Module (VEM), offering transparent firewall insertion and efficient deployment. All the policy management for VSG is done via Virtual Network Management Center (VNMC). Cisco VSG provides the following:

- Zone-based security controls based on network as well as virtual machine attributes. This flexibility simplifies security policies, which are easy to troubleshoot and audit.
- Secure multi-tenant deployment, protecting tenant workloads on a shared compute infrastructure.
- Leverages vPath intelligence for efficient network-wide deployment and accelerated performance through fast-path off-load.
- IT security, network, and server teams to collaborate while helping ensure administrative segregation to meet regulatory and audit requirements and reduce administrative errors.

Primary PCI Function

The main function of the Cisco VSG is segmentation of PCI scope and enforcement of that new scope boundary. The Cisco VSG serves as a stateful firewall, restricting traffic between the cardholder data environment and other areas of the network. (1.2, 1.3)

Table 5-59 PCI Assessment Summary—Cisco VSG

Models Assessed	
Nexus VSG version 4.2(1)VSG1(1)	
PCI Sub-Requirements Passed	
PCI 1	1.2.1, 1.2.2, 1.3.5, 1.3.6, 1.3.7
PCI 2	2.2, 2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Table 5-59 lists the component assessment details for the Cisco VSG.

Table 5-60 Component Capability Assessment—Cisco VSG

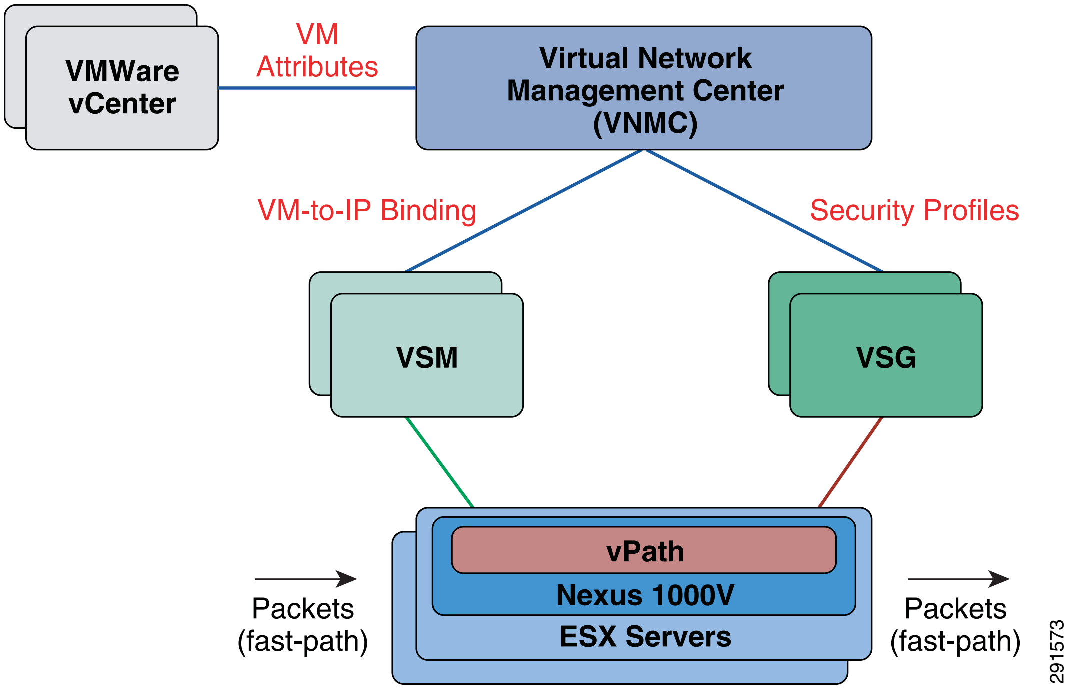
Cisco VSG	
PRIMARY FUNCTION	**Requirement 1 (1.2, 1.3)**
Restrict traffic between the cardholder data environment and other network areas.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

Cisco VSG integrates with Cisco Nexus 1000V Series Switches to enforce security policies for your virtualized environment. VNMC provides policy management for a multitenant environment. One or more VSGs are required per tenant. VSG uses the vPath intelligence in the Virtual Ethernet Module (VEM) of the Cisco Nexus 1000V Series to provide the security policy enforcement.

Cisco VSG is deployed as a virtual appliance in vCenter. The primary function of Cisco VSG is to protect against unauthorized access to the cardholder environment.

Figure 5-113 Cisco Nexus VSG System Architecture



PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

Cisco VSG can protect the cardholder data environment from untrusted networks by enforcing security policies for any network traffic entering or leaving a virtual machine. These security policies are enabled at a port-profile level in the Cisco Nexus 1000V. All the virtual machines connecting to the network with those port-profiles (port-groups) are protected through firewall policies.

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*
- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of devices are synchronized.
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*

- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*

To insert the firewall into the network, you need to attach the security profile to the port profile. All the traffic traversing through the virtual ports associated with that port profile, is enforced by the security policy. The following two commands enable the firewall feature under the port profile:

```
Nexus1000V (config)# org root/TenantA
Nexus1000V (config)# vn-service ip-address VSG_Data_IP vlan VSG_Service_VLAN
security-profile SecureTenantA
```

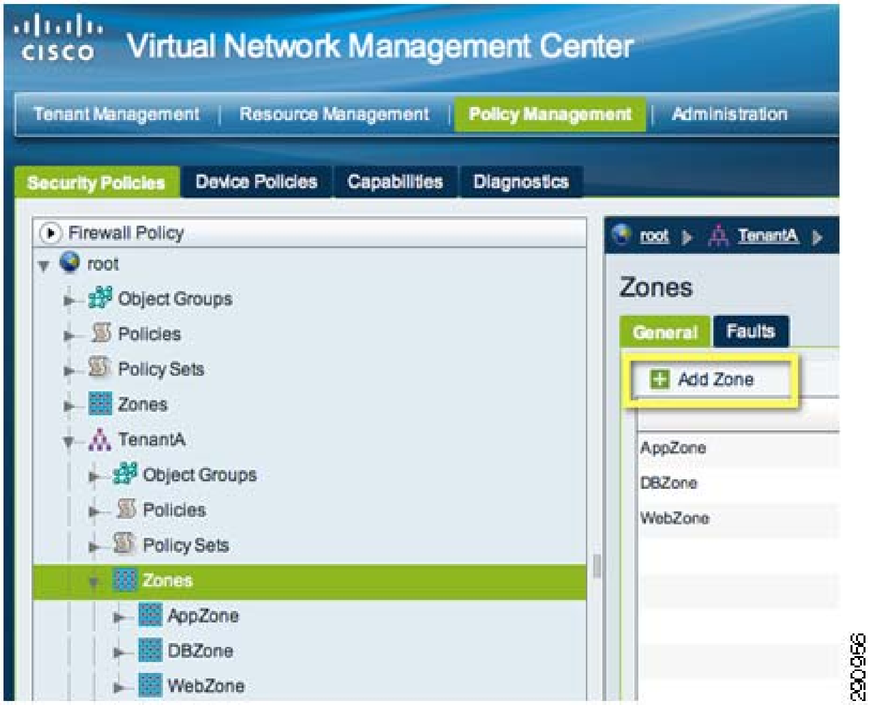
The first command specifies the tenant whose workload is being protected. The second command binds the security profile to the port-profile for that tenant. Once the firewall is enabled, the traffic is intercepted by vPath and sent to Cisco VSG over a dedicated VLAN. Cisco VSG evaluates the traffic against the security policy. It sends the decision (deny or allow) back to vPath, which enforces the Cisco VSG decision to the traffic flow. VNMC publishes the security policies for each tenant for individual Cisco VSGs. These policies are maintained and edited in the VNMC.

Placing cardholder data systems in security zones can isolate the environment from the DMZ and external network. These zones are leveraged in writing the security policies in the VNMC.

To create the Navigation pane, do the following:

1. Click the Policy Management tab, click the Security Policies subtab, and expand Firewall Policy > root to view the appropriate Zones node.
2. Select the organizational level (Tenant) where you want to add the zone. In the Work pane, click the Add Zone link. (See Figure 5-114.)

Figure 5-114 Virtual Network Management Center—Policy Management



Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Nexus VSG does not have any unnecessary services enabled by default.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Only SSH access is allowed for firewall console access over the network. The communication between Cisco VSG and Management Platform (VNMC) is all encrypted over SSL (443)

  Cisco Nexus VSG can be configured to use secure protocols for all system functions. This includes SSH for remote management, SCP, and SFTP for file transfers. Insecure services can be disable or blocked using configuration statements and access lists.

  ```
  no feature telnet
  no telnet server enable
  feature ssh
  ```

  Cisco Nexus VSG support administrative protocols with strong cryptography such as SSH version 2.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Nexus Virtual Security Gateway. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by the Cisco Nexus VSG using LDAP services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*

- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

User roles in VNMC contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has policy-related privileges, and Role2 has tenant-related privileges, users who are assigned to both Role1 and Role2 have policy and tenant related privileges.

The system contains the following default user roles:

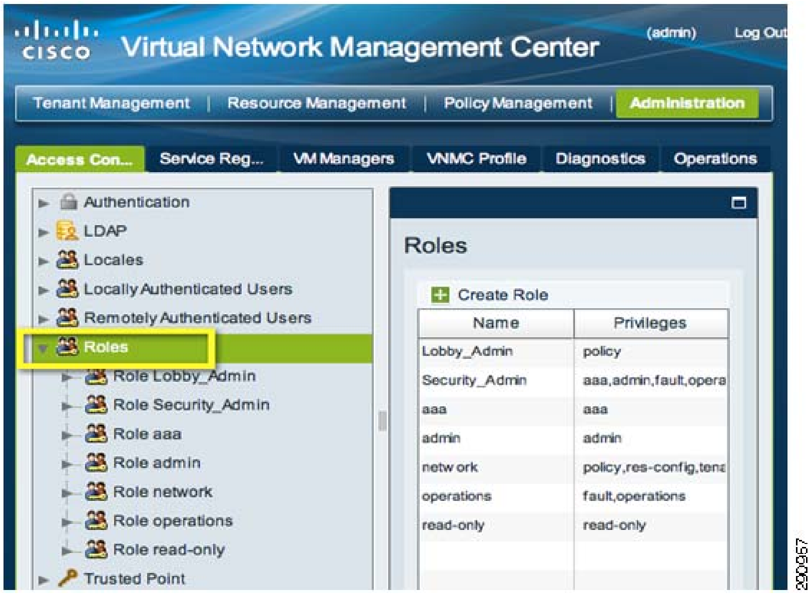
- aaa—User has read and write access to users, roles, and AAA configuration. Read access to the rest of the system.
- admin—User has complete read-and-write access to the entire system and has all privileges. The default admin account is assigned this role by default, and it cannot be changed.
- network—User creates organizations, security policies, and device profiles.
- operations—User acknowledges faults and performs some basic operations such as logging configuration.
- read-only—User has read-only access to system configuration and operational status with no privileges to perform any operations.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Network and Operations roles have different sets of privileges, but a new Network and Operations role can be created that combines the privileges of both roles.

To configure roles in VNMC, do the following:

1. Click the **Administration** tab, then click the **Access Control** sub-tab.
2. In the Navigation pane, select the **Roles** node. In the Work pane, click **Create Roles** (see Figure 5-115.)

Figure 5-115 Configuring Roles

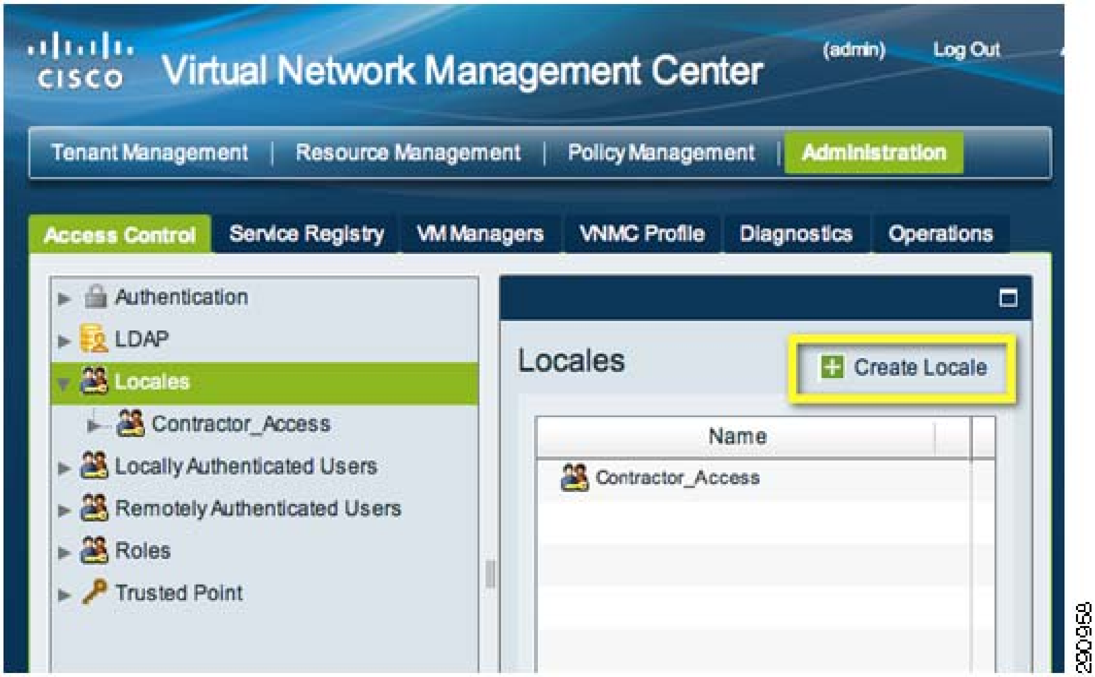


Name	Privileges
Lobby_Admin	policy
Security_Admin	aaa,admin,fault,opera
aaa	aaa
admin	admin
netw ork	policy,res-config,tena
operations	fault,operations
read-only	read-only

In addition to roles, the user is also provided another dimension of privilege, which limits the user to tenant level visibility, called *locale*. Each locale defines one or more organizations (domains) to which the user is allowed access, and access would be limited to the organizations specified in the locale. To configure locales in VNMC, do the following:

1. Click the Administration tab, then click the Access Control sub-tab.
2. In the Navigation pane, select the Locales node.
3. In the Work pane, click the Create Locale link. (See Figure 5-116.)

Figure 5-116 Configuring Locales



Name
Contractor_Access

CLI configuration of AAA services is as follows:

```
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
!
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the LDAP authentication capabilities to the Windows Active Directory server for AAA services. Microsoft Active Directory contains the necessary user account services for all of the appropriate PCI 8 requirements. Configure AAA services as shown above in Requirement 7.

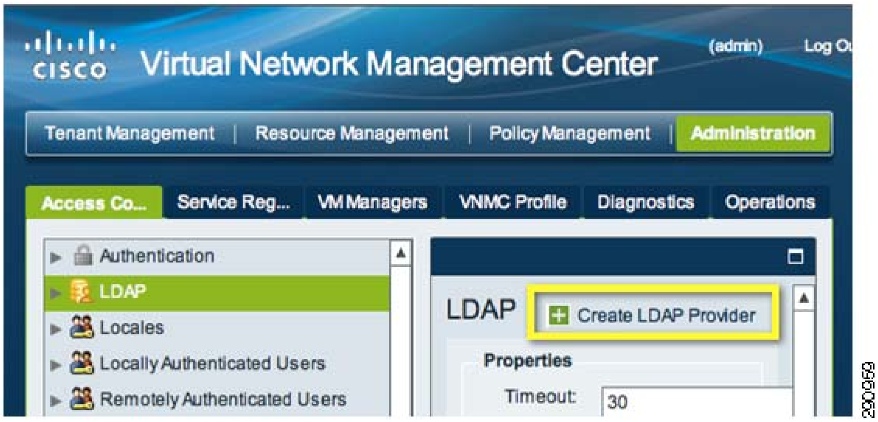
- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco VNMC provides remote authentication with LDAP servers for user authentication. When user accounts are created in the LDAP server, the accounts also include the roles and locales those users require for working in Cisco VNMC.

  To configure the LDAP server, do the following:

  1. Click the Administration tab, the click the Access Control sub-tab.
  2. In the Navigation pane, select the LDAP node.
  3. In the Work pane, click the Create LDAP Provider link. (See Figure 5-117.)

Figure 5-117 Configuring LDAP Server



Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco Nexus VSG is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Nexus VSG uses NTP to update and synchronize local clock facilities and meet the following requirements:

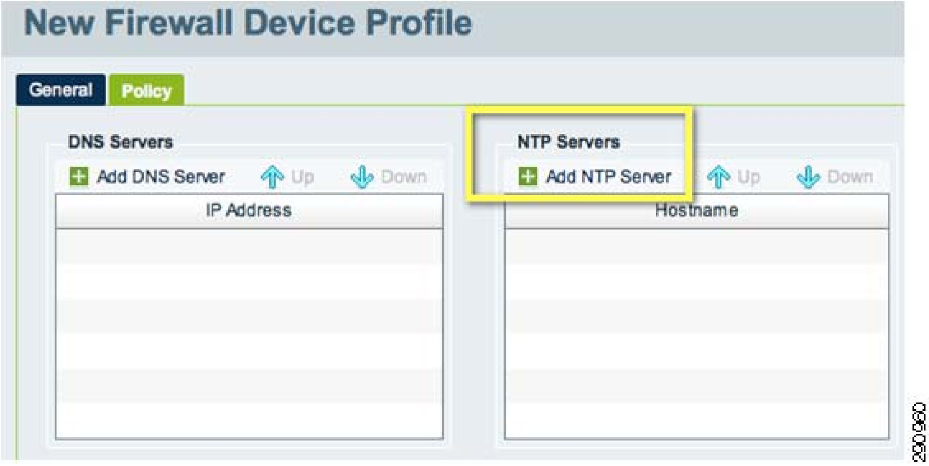
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

NTP is configured in the Firewall Device Profile for the Cisco VSG VNMC. The setting is published via the device policy to Cisco VSG.

1. In the navigation pane, click the Policy Management tab, then the Device Policies sub-tab, and expand the Device Profile for a tenant.
2. Click a Profiles node to add a firewall device profile, and you see the option to add NTP server, as shown in Figure 5-118.

Figure 5-118 Configuring NTP



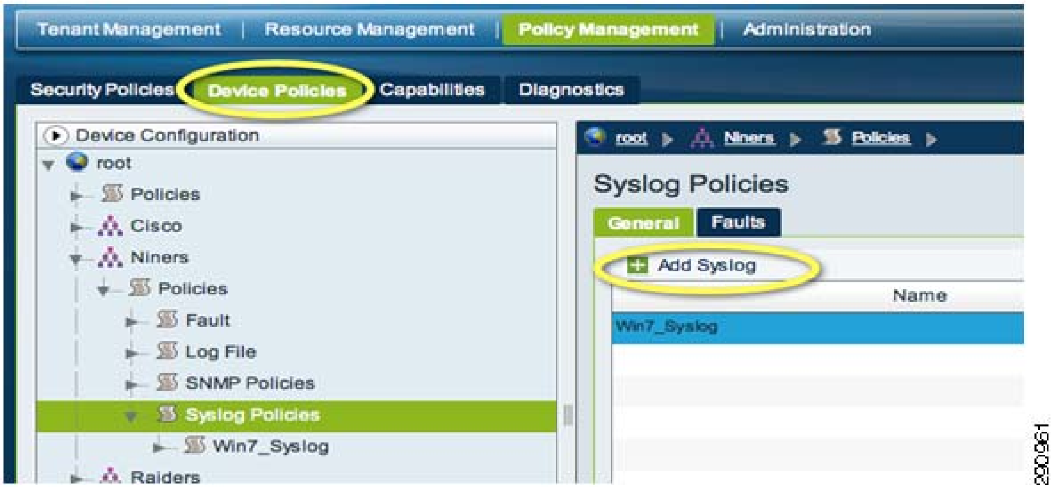
Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  You can configure the syslog server for Cisco VSG to send all the logging information to a standard syslog server. This setting is available as part of the device profile.

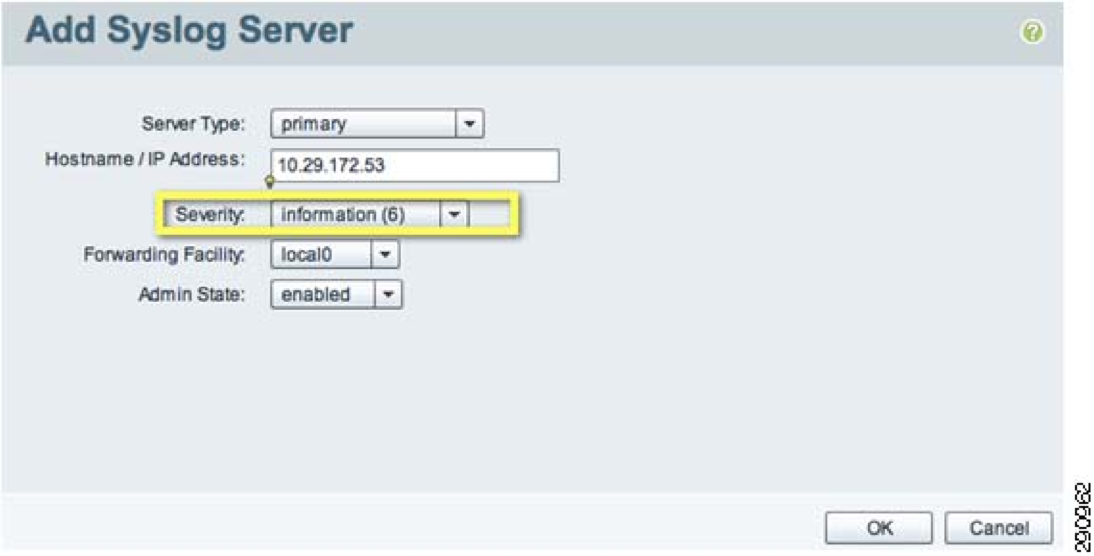
  1. Navigate to Policy Management > Device Policies > Tenant> Policies > Syslog Policies. Add a syslog policy, as shown in Figure 5-119.

Figure 5-119 Configuring Syslog



2. The severity of the logging should be at level 6 to capture the firewall policy hit in the VSG. (See Figure 5-120).

Figure 5-120 Configuring Logging Severity


Add Syslog Server

Server Type: primary
Hostname / IP Address: 10.29.172.53
Severity: information (6)
Forwarding Facility: local0
Admin State: enabled

3. The syslog policy is attached to the Device Profile to enable the settings in the VSG.

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

Intrusion Detection

Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2

The Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (IDSM2) is an important intrusion prevention system (IPS) solution that protects switched environments by integrating full-featured IPS functions directly into the network infrastructure through the widely deployed Cisco Catalyst chassis. This integration allows the user to monitor traffic directly off the switch backplane.

The Cisco IDSM-2 with Cisco IPS Sensor Software v6.0 helps users stop more threats with greater confidence, through the use of the following elements:

- Multivector threat identification—Detailed inspection of Layer 2–7 traffic protects your network from policy violations, vulnerability exploitations, and anomalous activity.
- Accurate prevention technologies—The innovative Cisco Risk Rating feature and Meta Event Generator provide the confidence to take preventive actions on a broader range of threats without the risk of dropping legitimate traffic.

When combined, these elements provide a comprehensive inline prevention solution, providing the confidence to detect and stop the broadest range of malicious traffic before it affects business continuity.

Table 5-61 PCI Assessment Summary—Cisco IDSM2

Models Assessed	
WS-SVC-IDSM-2 version 7.0(4)	
PCI Sub-Requirements Passed	
PCI 2	2.2.2, 2.2.4, 2.3
PCI 6	6.1
PCI 7	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3
PCI 8	8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15
PCI 10	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3
PCI 11	11.4
PCI Sub-Requirements Requiring Compensating Controls	
No compensating controls were required to satisfy any sub-requirements.	
PCI Sub-Requirements Failed	
No sub-requirements were failed.	

Primary PCI Function

The primary PCI function of the Cisco ISDM2 is to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises (11.4).

Table 5-61 lists the component assessment details for the Cisco ISDM2.

Table 5-62 Component Capability Assessment—Cisco ISDM2

Cisco IDSM2	
PRIMARY FUNCTION	**Requirement 11 (11.4)**
Monitor all traffic at the perimeter of the CDE as well as at critical points inside the CDE.	
CAPABILITY	**ASSESSMENT**
Secure Services	
Disabled any unnecessary services—*"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)	●
Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)	●
Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)	●
Authentication	
Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)	◉
Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)	◉
Logs	
Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)	◉
The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)	●

Design Considerations

- Configure the Cisco IDSM2 to lock accounts so that users cannot keep trying to login after a certain number of failed attempts.
- Allow secure management of the Cisco IDSM2 only from a specific host/hosts.
- Configure appropriate banner messages on login. The login banner warning should not reveal the identity of the company that owns or manages the Cisco IDSM2. The banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Change default passwords and community strings to appropriate complexity.

For more information, see the Installation Guide at the following URL:
http://www.cisco.com/en/US/docs/security/ips/6.0/configuration/guide/cli/cliInter.html

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

Cisco IDSM2 modules allow only administrative connections from authorized hosts/networks as specified in the device configuration. The following configuration shows the authorized management hosts for SSH and HTTPS administration, and disabling of Telnet.

```
! -----------------------------
service host
network-settings
host-ip 192.168.21.94/24,192.168.21.1
host-name DMZ-IDS2
telnet-option disabled
access-list 10.19.151.99/32
access-list 192.168.41.101/32
access-list 192.168.41.102/32
access-list 192.168.42.122/32
access-list 192.168.42.124/32
access-list 192.168.42.133/32
access-list 192.168.42.138/32
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco IDSM2 modules do not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco IDSM2 modules use strong encryption for SSH and HTTPS.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco IDSM2 modules. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS RADIUS services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*

- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco IDSM2 modules are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements use the RADIUS protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
! -----------------------------
service aaa
aaa radius
primary-server
server-address 192.168.42.131
shared-secret <removed>
exit
nas-id DMZ-IDS1
local-fallback enabled
console-authentication radius-and-local
default-user-role administrator
exit
exit
! -----------------------------
```

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services, as shown above in Requirement 7.

The Cisco IDSM2 module is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco IDSM2 modules support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

```
sensor(config)# username username password password privilege
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something yo*u are, such as a biometric

  When configuring local user accounts, you must specify a password to achieve PCI compliance.
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  All local passwords on the Cisco IDSM2 are stored using strong encryption.
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

Cisco IDSM2 modules do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco IDSM2 modules do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco IDSM2 modules support the ability to specify a minimum password length for local accounts.

```
! -----------------------------
service authentication
password-strength
size 7-64
! -----------------------------
```

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco IDSM2 modules support the ability to specify alphanumeric passwords for local accounts.

```
! -----------------------------
service authentication
password-strength
digits-min 1
lowercase-min 1
other-min 1
! -----------------------------
```

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco IDSM2 modules support the ability to specify that old passwords should not be re-used for local accounts.

```
! -----------------------------
service authentication
password-strength
number-old-passwords 4
! -----------------------------
```

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco IDSM2 modules support the ability to specify that only a limited number of attempts can be made when authenticating for local accounts.

```
! -----------------------------
service authentication
attemptLimit 6
! -----------------------------
```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco IDSM2 modules support the ability to lockout local accounts after the specified number of failed attempts, requiring an administrator to re-enable them. Locked accounts are indicated by parentheses when using the **show users** command:

```
sensor# show users all
    CLI ID   User         Privilege
*   1349     bart         administrator
```

```
5824     (pauljones)  viewer
9802     christian    operator
```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco IDSM2 modules do not feature an explicit session timeout. Administration time limits would need to be enabled systemically through active directory policy to the admin workstation desktops.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco IDSM2 is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco IDSM2 uses NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco IDSM2 uses NTP to meet these requirements by implementing the following configuration statements:

  ```
  time-zone-settings
  offset -8
  standard-time-zone-name PST
  exit
  ntp-option enabled-ntp-unauthenticated
  ntp-server 192.168.62.161
  exit
  summertime-option recurring
  ```

```
summertime-zone-name PDT
```

To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Note The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco IDSM2 modules are capable of sending system events to a centralized repository using SNMP traps. Logs stored locally are buffered and require operator level privileges on the device to be viewed. External logging is enabled by implementing the following configuration statements to send them to the RSA enVision server:

```
! ------------------------------
service notification
trap-destinations 192.168.42.124
trap-community-name RSAenVision
exit
enable-notifications true
trap-community-name RSAenVision
exit
! ------------------------------
```

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.4**—*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.*

  Cisco IDSM2 modules are capable of performing intrusion detection and prevention through the use of VLAN interfaces from the host Cisco Catalyst service chassis. IPS signature updates and configurations are managed centrally through Cisco Security Manager. The following configuration statements are necessary in the Cisco Catalyst service chassis to forward traffic via VLANs and enable the IDS inspection capability:

```
!
!
intrusion-detection module 2 management-port access-vlan 21
intrusion-detection module 2 data-port 1 trunk allowed-vlan 83,84
!
```

Cisco IDSM2 module interfaces are configured as follows to receive, inspect, and forward traffic across the assigned VLANs:

```
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/7
subinterface-type inline-vlan-pair
subinterface 1
description INT1 vlans 83 and 84
vlan1 83
vlan2 84
exit
exit
exit
exit
! ------------------------------
```

PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

CHAPTER 6

Summary

PCI can be simplified. Moreover, enterprise-class retailing can be simplified. The Cisco Connected Retail Architecture provides the core infrastructure and principles for minimizing the complexity of running large-scale organizations. When combined with Cisco's strategic partners, compliance challenges are met with a comprehensive and unique approach that stands alone in the industry.

Compliance is a journey, not a destination. It requires continual attention to maintain. It is a journey that cannot be traveled alone. Trusted advisors such as auditors and vendors simplify the goal of maintaining compliance. Table 6-1 provides a summary of the PCI assessment results.

Table 6-1 PCI Assessment Results Summary

Component	Primary PCI Function		Component	Primary PCI Function
Endpoints and Applications			**Infrastructure**	
Cisco UCM and IP Phones	9.1.2		Cisco store routers	1.3, 11.4
Video Surveillance	9.1.1		Cisco data center routers	1.2, 1.3
Cisco Physical Access Control	9.1		Cisco store switches	9.1.2, 11.1b, 11.1d Segmentation
Cisco IronPort Email Security Solutions	DLP		Cisco data center switches	1.2, 1.3, 11.4
Cisco UCS	Servers		Cisco Nexus 1000V Series Switch	Segmentation
UCS Express on Cisco SRE	Servers		Cisco Nexus data center switches	Segmentation
Scope Administration			Cisco Wireless	4.1, 11.1
Cisco ACS	7.1		Cisco MDS Switch	3.4
RSA Authentication Manager	8.3		Cisco ASA-store	1.3, 11.4
HyTrust Appliance	10.5		Cisco ASA-data center	1.3, 11.4
Cisco Security Manager	1.2		Cisco FWSM-data center	1.3
EMC Ionix NCM	1.2.2		Cisco Nexus VSG	Virtual firewall
RSA Data Protection Manager	3.5		IDSM-data center	11.4
EMC CLARiioN	Storage		Cisco TrustSec	7.1, 11.1b, 11.1d
RSA enVision	10.5			

APPENDIX A

Bill Of Material

Store—MSP Store

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	5
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	Cisco 1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	5
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	5
CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	Cisco SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	5
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	5
AIR-WLC2125-K9	AIR-WLC2125-K9	Cisco	Cisco 2100 Series WLAN Controller for up to 25 Lightweight APs	1
ASA5505-PWR-AC	ASA5505-PWR-AC	Cisco	Cisco ASA 5505 AC Power Supply Adapter	1
SSC-BLANK	SSC-BLANK	Cisco	Cisco ASA 5505 SSC Blank Slot Cover	1
SWLC2100K9-70-ER	SWLC2100K9-70-ER	Cisco	Cisco Unified Wireless Controller SW Release 7.0	1
CAB-AC-C5	CAB-AC-C5	Cisco	AC Power Cord, Type C5, US	1
CON-SNT-AC2125K9	CON-SNT-AC2125K9	Cisco	SMARTNET 8X5XNBD WLAN Controller for for Retail	1
SWLC2100K9-70	SWLC2100K9-70	Cisco	Cisco Unified Wireless Controller SW Release 7.0	1

ASA5510-AIP10SP-K9	ASA5510-AIP10SP-K9	Cisco	Cisco ASA 5510 with AIP-SSM-10, 2GE+3FE, SW, HA,3DES/AES, SEC PLUS	1
ASA5510-SEC-PL	ASA5510-SEC-PL	Cisco	Cisco ASA 5510 Security Plus License w/ HA, GE, more VLANs + conns	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-NSST-AS1A1PK9	CON-NSST-AS1A1PK9	Cisco	NOS 8X5XNBD ASA5510-AIP10SP-K9	1
SF-ASA-8.3-K8	SF-ASA-8.3-K8	Cisco	Cisco ASA 5500 Series Software v8.3	1
SF-ASA-AIP-7.0-K9	SF-ASA-AIP-7.0-K9	Cisco	Cisco ASA 5500 Series AIP Sofware 7.0 for Security Service Modules	1
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	1
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	1
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	1

CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	1
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	1
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	1
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	1
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	1
CIVS-MSP-1RU	CIVS-MSP-1RU	Cisco	1RU MSP Assembly	1
CIVS-CAB-16-AC	CIVS-CAB-16-AC	Cisco	CIVS C16 Power Cable North America	1
CIVS-HDD-1000	CIVS-HDD-1000	Cisco	1TB SATA Drive for CIVS-MSP	4
CIVS-MS-SW6.2	CIVS-MS-SW6.2	Cisco	CIVS-MS Media Server v6.2 Software License with Hardware	1
CIVS-VSM-SW4262	CIVS-VSM-SW4262	Cisco	CIVS-VSM Video Surveillance Manager v4.2/6.2 SW Mfg Image	1
CON-SNT-VSM1U	CON-SNT-VSM1U	Cisco	SMARTNET 8X5XNBD 1RU MSP Assembly	1
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	1
CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	1
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C2960S-48FPS-L	WS-C2960S-48FPS-L	Cisco	Catalyst 2960S 48 GigE PoE 740W, 4 x SFP LAN Base	1
CAB-L620P-C13-US	CAB-L620P-C13-US	Cisco	Power Cord, 250VAC, 15A, NEMA L6-20 to C13, US	1

Store—Convenience Store

Name	Catalog Num	Vendor	Description	Qty
AIR-LAP1042N-A-K9	AIR-LAP1042N-A-K9	Cisco	802.11a/g/n Fixed Unified AP; Int Ant; A Reg Domain	1
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	1
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	1
CON-SNT-L1042A	CON-SNT-L1042A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Fixed Un	1
S104RK9W-12423JA	S104RK9W-12423JA	Cisco	Cisco 1040 Series IOS WIRELESS LAN LWAPP RECOVERY	1
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	1
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	1
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	1
CISCO891W-AGN-A-K9	CISCO891W-AGN-A-K9	Cisco	Cisco 891 GigaE SecRouter w/ 802.11n a/b/g FCC Comp	1
AIR-ANTM2050D-R	AIR-ANTM2050D-R	Cisco	2.2dBi/2.4Ghz,5.0dBi/5GHz DualBand Dipole Antenna	3
CAB-AC2	CAB-AC2	Cisco	AC Power cord North America	1
CAB-ETH-S-RJ45	CAB-ETH-S-RJ45	Cisco	Yellow Cable for Ethernet, Straight-through, RJ-45, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-80W-AC	PWR-80W-AC	Cisco	Power Supply 80 Watt AC	1
S890VK9-15001M	S890VK9-15001M	Cisco	Cisco 890 Series IOS UNIVERSAL	1
SL-890-AIS	SL-890-AIS	Cisco	Cisco 890 Advanced IP Services License	1
800-IL-PM-4	800-IL-PM-4	Cisco	4 Port 802.3af capable pwr module for 890 Series Router	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-C891WAK9	CON-SNT-C891WAK9	Cisco	SMARTNET 8X5XNBD Cisco 891 GigaE SecRouter	1
MEM8XX-512U768D	MEM8XX-512U768D	Cisco	DRAM Upgrade 512 MB to 768 MB	1

CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
WS-C2960PD-8TT-L	WS-C2960PD-8TT-L	Cisco	Catalyst 2960 Powered Device 8 10/100 + 1 1000BT LAN Base	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-C2960P8T	CON-SNT-C2960P8T	Cisco	SMARTNET 8X5XNBD Cat2960 Pwrd Device 8 10/100-1 1K BT LAN	1
PWR-A	PWR-A	Cisco	Pwr Sply In:100-240VAC Out:48VDC 380mA-2960PD-8TT-L	1

Stores—Mini Store

Name	Catalog Num	Vendor	Description	Qty
AIR-LAP1042N-A-K9	AIR-LAP1042N-A-K9	Cisco	802.11a/g/n Fixed Unified AP; Int Ant; A Reg Domain	1
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	1
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	1
CON-SNT-L1042A	CON-SNT-L1042A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Fixed Un	1
S104RK9W-12423JA	S104RK9W-12423JA	Cisco	Cisco 1040 Series IOS WIRELESS LAN LWAPP RECOVERY	1
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	1
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	1
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	1

CISCO1941W-A/K9	CISCO1941W-A/K9	Cisco	Cisco 1941 Router w/ 802.11 a/b/g/n FCC Compliant WLAN ISM	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
S801RK9W-12421JA	S801RK9W-12421JA	Cisco	Cisco 801 Series IOS WIRELESS LAN LWAPP RECOVERY	1
S801W7K9-12421JA	S801W7K9-12421JA	Cisco	Cisco 801 Series IOS WIRELESS LAN	1
SL-19-IPB-K9	SL-19-IPB-K9	Cisco	IP Base License for Cisco 1900	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-1941WA	CON-SNT-1941WA	Cisco	SMARTNET 8X5XNBD Cisco 1941 Router w/ 802.11 a/b/g/n FCC	1
HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
MEM-1900-512U2.5GB	MEM-1900-512U2.5GB	Cisco	512MB to 2.5GB DRAM Upgrade (2GB+512MB) for Cisco 1941 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
PWR-1941-POE	PWR-1941-POE	Cisco	Cisco 1941 AC Power Supply with Power Over Ethernet	1
S19UK9-15102T	S19UK9-15102T	Cisco	Cisco 1900 IOS UNIVERSAL	1
SL-19-SEC-K9	SL-19-SEC-K9	Cisco	Security License for Cisco 1900	1
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
WS-C2960G-8TC-L	WS-C2960G-8TC-L	Cisco	Cisco Catalyst 2960 7 10/100/1000 + 1 T/SFP LAN Base	2

CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	2
CON-SNT-C2960G8C	CON-SNT-C2960G8C	Cisco	SMARTNET 8X5XNBD Catalyst 2960 7 10/1	2
GLC-SX-MM=	GLC-SX-MM=	Cisco	GE SFP, LC connector SX transceiver	2
PWR-CLIP	PWR-CLIP	Cisco	Power retainer clip for compact switches	2
RCKMNT-19-CMPCT=	RCKMNT-19-CMPCT=	Cisco	19in RackMount for Cisco Catalyst 3560,2960,ME-3400 Compact Switch	2

Stores—Small Store

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502E-A-K9	AIR-CAP3502E-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Ext Ant; A Reg Domain	2
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	2
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	2
AIR-ANT2422DW-R	AIR-ANT2422DW-R	Cisco	2.4 GHz 2.2 dBi Swivel Dipole Antenna White, RP-TNC	6
AIR-ANT5135DW-R	AIR-ANT5135DW-R	Cisco	5 GHz 3.5 dBi Swivel Dipole Antenna White, RP-TNC	6
CON-SNT-CAP3502A	CON-SNT-CAP3502A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; E	2
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	2
AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	2
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	2
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	2
CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	2
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	2
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	2
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	2

CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	2
CISCO2921-SEC/K9	CISCO2921-SEC/K9	Cisco	Cisco 2921 Security Bundle w/SEC license PAK	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-2921-51-AC	PWR-2921-51-AC	Cisco	Cisco 2921/2951 AC Power Supply	1
SL-29-IPB-K9	SL-29-IPB-K9	Cisco	IP Base License for Cisco 2901-2951	1
SL-29-SEC-K9	SL-29-SEC-K9	Cisco	Security License for Cisco 2901-2951	1
SM-DSK-SATA-500GB	SM-DSK-SATA-500GB	Cisco	500 GB hard disk drive for SRE SM	2
SM-MEM-VLP-2GB	SM-MEM-VLP-2GB	Cisco	2GB Very Low Profile SDRAM for SRE SM	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-2921SEC	CON-SNT-2921SEC	Cisco	SMARTNET 8X5XNBD Cisco 2921 Security	1
DISK-MODE-RAID-0	DISK-MODE-RAID-0	Cisco	Configure hard drives as RAID 0	1
FL-VMSS-SM-MS	FL-VMSS-SM-MS	Cisco	Video Management and Storage System Media Server License	1
FL-VMSS-SM-OM	FL-VMSS-SM-OM	Cisco	Video Management and Storage System Operations Manager Licen	1
HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
MEM-2900-512U2.5GB	MEM-2900-512U2.5GB	Cisco	512MB to 2.5GB DRAM Upgrade (2GB+512MB) for Cisco 2901-2921	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
S29UK9-15102T	S29UK9-15102T	Cisco	Cisco 2901-2921 IOS UNIVERSAL	1
SM-SRE-900-K9	SM-SRE-900-K9	Cisco	Services Module with Services Ready Engine (SRE)	1
SM-VMSS-6.2.1-K9	SM-VMSS-6.2.1-K9	Cisco	Video Management and Storage System Software 6.2.1for the SM	1
SM9-VMSS	SM9-VMSS	Cisco	VMSS software contrainer for SM-SRE-900-K9	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1

CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	1
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	1
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	1
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	1
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	1
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	1
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	1
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	1

CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	1
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C2960S-48FPS-L	WS-C2960S-48FPS-L	Cisco	Cisco Catalyst 2960S 48 GigE PoE 740W, 4 x SFP LAN Base	1
CAB-L620P-C13-US	CAB-L620P-C13-US	Cisco	Power Cord, 250VAC, 15A, NEMA L6-20 to C13, US	1

Stores—Medium Store

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502E-A-K9	AIR-CAP3502E-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Ext Ant; A Reg Domain	7
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	7
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	7
AIR-ANT2422DW-R	AIR-ANT2422DW-R	Cisco	2.4 GHz 2.2 dBi Swivel Dipole Antenna White, RP-TNC	21
AIR-ANT5135DW-R	AIR-ANT5135DW-R	Cisco	5 GHz 3.5 dBi Swivel Dipole Antenna White, RP-TNC	21
CON-SNT-CAP3502A	CON-SNT-CAP3502A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; E	7
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	7
AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	7
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	7
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	7
CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	7
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	7
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4

CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CISCO2951-SEC/K9	CISCO2951-SEC/K9	Cisco	Cisco 2951 Security Bundle w/SEC license PAK	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-2921-51-AC	PWR-2921-51-AC	Cisco	Cisco 2921/2951 AC Power Supply	1
SL-29-IPB-K9	SL-29-IPB-K9	Cisco	IP Base License for Cisco 2901-2951	1
SL-29-SEC-K9	SL-29-SEC-K9	Cisco	Security License for Cisco 2901-2951	1
SM-DSK-SATA-500GB	SM-DSK-SATA-500GB	Cisco	500 GB hard disk drive for SRE SM	2
SM-MEM-VLP-2GB	SM-MEM-VLP-2GB	Cisco	2GB Very Low Profile SDRAM for SRE SM	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
DISK-MODE-RAID-0	DISK-MODE-RAID-0	Cisco	Configure hard drives as RAID 0	1
FL-VMSS-SM-MS	FL-VMSS-SM-MS	Cisco	Video Management and Storage System Media Server License	1
FL-VMSS-SM-OM	FL-VMSS-SM-OM	Cisco	Video Management and Storage System Operations Manager Licen	1
HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
MEM-2951-512U2GB	MEM-2951-512U2GB	Cisco	512MB to 2GB DRAM Upgrade (1 2GB DIMM) for Cisco 2951 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
S2951UK9-15102T	S2951UK9-15102T	Cisco	Cisco 2951 IOS UNIVERSAL	1
SM-SRE-900-K9	SM-SRE-900-K9	Cisco	Services Module with Services Ready Engine (SRE)	1
SM-VMSS-6.2.1-K9	SM-VMSS-6.2.1-K9	Cisco	Video Management and Storage System Software 6.2.1for the SM	1
SM9-VMSS	SM9-VMSS	Cisco	VMSS software contrainer for SM-SRE-900-K9	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CISCO2951-SEC/K9	CISCO2951-SEC/K9	Cisco	Cisco 2951 Security Bundle w/SEC license PAK	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-2921-51-AC	PWR-2921-51-AC	Cisco	Cisco 2921/2951 AC Power Supply	1

SL-29-IPB-K9	SL-29-IPB-K9	Cisco	IP Base License for Cisco 2901-2951	1
SL-29-SEC-K9	SL-29-SEC-K9	Cisco	Security License for Cisco 2901-2951	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
MEM-2951-512U2GB	MEM-2951-512U2GB	Cisco	512MB to 2GB DRAM Upgrade (1 2GB DIMM) for Cisco 2951 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
NME-AIR-WLC25-K9	NME-AIR-WLC25-K9	Cisco	25-AP WLAN Controller NM for Cisco 2800/3800 Series	1
S2951UK9-15102T	S2951UK9-15102T	Cisco	Cisco 2951 IOS UNIVERSAL	1
SM-NM-ADPTR	SM-NM-ADPTR	Cisco	Network Module Adapter for SM Slot on Cisco 2900, 3900 ISR	1
SWLCEK9-60	SWLCEK9-60	Cisco	Cisco Unified WLAN Controller SW Release 6.0 - MD	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	2
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	2
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	2
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	2
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	2
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	2
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	2
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	2
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	2
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1

CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	2
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	2
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	2
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	2
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	2
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	2
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	2
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	2
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	2
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	1
CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	1
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C2960PD-8TT-L	WS-C2960PD-8TT-L	Cisco	Cisco Catalyst 2960 Powered Device 8 10/100 + 1 1000BT LAN Base	10
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	10
CON-SNT-C2960P8T	CON-SNT-C2960P8T	Cisco	SMARTNET 8X5XNBD Cat2960 Pwrd Device 8 10/100-1 1K BT LAN	10
PWR-A	PWR-A	Cisco	Pwr Sply In:100-240VAC Out:48VDC 380mA-2960PD-8TT-L	10
WS-C3750X-48PF-S	WS-C3750X-48PF-S	Cisco	Cisco Catalyst 3750X 48 Port Full PoE IP Base	2
C3KX-PWR-1100WAC	C3KX-PWR-1100WAC	Cisco	Cisco Catalyst 3K-X 1100W AC Power Supply	2
C3KX-NM-1G	C3KX-NM-1G	Cisco	Cisco Catalyst 3K-X 1G Network Module option PID	2

C3KX-PWR-1100WAC/2	C3KX-PWR-1100WAC/2	Cisco	Cisco Catalyst 3K-X 1100W AC Secondary Power Supply	2
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	4
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	2
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	2
CON-SNT-3750X4FS	CON-SNT-3750X4FS	Cisco	SMARTNET 8X5XNBD Catalyst 3750X 48 Port Full PoE IP Base	2
S375XVK9T-12253SE	S375XVK9T-12253SE	Cisco	Cisco CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	2
SFP-GE-S=	SFP-GE-S=	Cisco	1000BASE-SX SFP (DOM)	8

Stores—Large Store

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502E-A-K9	AIR-CAP3502E-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Ext Ant; A Reg Domain	12
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	12
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	12
AIR-ANT2422DW-R	AIR-ANT2422DW-R	Cisco	2.4 GHz 2.2 dBi Swivel Dipole Antenna White, RP-TNC	36
AIR-ANT5135DW-R	AIR-ANT5135DW-R	Cisco	5 GHz 3.5 dBi Swivel Dipole Antenna White, RP-TNC	36
CON-SNT-CAP3502A	CON-SNT-CAP3502A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; E	12
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	12
AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	12
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	12
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	12
CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	12
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	12

AIR-CT5508-25-K9	AIR-CT5508-25-K9	Cisco	Cisco 5508 Series Wireless Controller for up to 25 APs	2
LIC-CT5508-25	LIC-CT5508-25	Cisco	25 AP Base license	2
LIC-CT5508-BASE	LIC-CT5508-BASE	Cisco	Base Software License	2
AIR-PWR-5500-AC	AIR-PWR-5500-AC	Cisco	Cisco 5500 Series Wireless Controller Redundant Power Supply	2
AIR-PWR-CORD-NA	AIR-PWR-CORD-NA	Cisco	AIR Line Cord North America	4
CON-SNT-CT0825	CON-SNT-CT0825	Cisco	SMARTNET 8X5XNBD Cisco 5508 Series	2
GLC-T=	GLC-T=	Cisco	1000BASE-T SFP	6
SWC5500K9-70	SWC5500K9-70	Cisco	Cisco Unified Wireless Controller SW Release 7.0	2
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	8
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	8
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	8
CISCO3945-SEC/K9	CISCO3945-SEC/K9	Cisco	Cisco 3945 Security Bundle w/SEC license PAK	1
3900-FANASSY	3900-FANASSY	Cisco	Cisco 3925/3945 Fan Assembly (Bezel included)	1
C3900-SPE150/K9	C3900-SPE150/K9	Cisco	Cisco Services Performance Engine 150 for Cisco 3945 ISR	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-3900-AC	PWR-3900-AC	Cisco	Cisco 3925/3945 AC Power Supply	1
SL-39-IPB-K9	SL-39-IPB-K9	Cisco	IP Base License for Cisco 3925/3945	1
SL-39-SEC-K9	SL-39-SEC-K9	Cisco	Security License for Cisco 3900 Series	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	2
CON-P2ST-NMEIPSK9	CON-P2ST-NMEIPSK9	Cisco	PM2, 8X5XNBD NME-IPS-K9	1
CON-SNT-3945SEC	CON-SNT-3945SEC	Cisco	SMARTNET 8X5XNBD Cisco 3945 Security Bundle w/SEC license	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
IPS-SW-NME-7.0-K9	IPS-SW-NME-7.0-K9	Cisco	IPS Software v7.0 for NME-IPS	1
MEM-3900-1GU2GB	MEM-3900-1GU2GB	Cisco	1GB to 2GB DRAM Upgrade (1GB+1GB) for Cisco 3925/3945 ISR	1

MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
NME-IPS-K9	NME-IPS-K9	Cisco	Cisco IPS NM for 2811, 2821, 2851 and 3800	1
PWR-3900-AC/2	PWR-3900-AC/2	Cisco	Cisco 3925/3945 AC Power Supply (Secondary PS)	1
S39UK9-15102T	S39UK9-15102T	Cisco	Cisco 3925-3945 IOS UNIVERSAL	1
SM-NM-ADPTR	SM-NM-ADPTR	Cisco	Network Module Adapter for SM Slot on Cisco 2900, 3900 ISR	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CISCO3945-SEC/K9	CISCO3945-SEC/K9	Cisco	Cisco 3945 Security Bundle w/SEC license PAK	1
3900-FANASSY	3900-FANASSY	Cisco	Cisco 3925/3945 Fan Assembly (Bezel included)	1
C3900-SPE150/K9	C3900-SPE150/K9	Cisco	Cisco Services Performance Engine 150 for Cisco 3945 ISR	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-3900-AC	PWR-3900-AC	Cisco	Cisco 3925/3945 AC Power Supply	1
SL-39-IPB-K9	SL-39-IPB-K9	Cisco	IP Base License for Cisco 3925/3945	1
SL-39-SEC-K9	SL-39-SEC-K9	Cisco	Security License for Cisco 3900 Series	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	2
CON-P2ST-NMEIPSK9	CON-P2ST-NMEIPSK9	Cisco	PM2, 8X5XNBD NME-IPS-K9	1
CON-SNT-3945SEC	CON-SNT-3945SEC	Cisco	SMARTNET 8X5XNBD Cisco 3945 Security Bundle w/SEC license	1
HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
IPS-SW-NME-7.0-K9	IPS-SW-NME-7.0-K9	Cisco	IPS Software v7.0 for NME-IPS	1
MEM-3900-1GU2GB	MEM-3900-1GU2GB	Cisco	1GB to 2GB DRAM Upgrade (1GB+1GB) for Cisco 3925/3945 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
NME-IPS-K9	NME-IPS-K9	Cisco	Cisco IPS NM for 2811, 2821, 2851 and 3800	1
PWR-3900-AC/2	PWR-3900-AC/2	Cisco	Cisco 3925/3945 AC Power Supply (Secondary PS)	1

S39UK9-15102T	S39UK9-15102T	Cisco	Cisco 3925-3945 IOS UNIVERSAL	1
SM-NM-ADPTR	SM-NM-ADPTR	Cisco	Network Module Adapter for SM Slot on Cisco 2900, 3900 ISR	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	4
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	4
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	4
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	4
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	4
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	4
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	4
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	4
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	4
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	4
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	4

CIVS-MSP-2RU	CIVS-MSP-2RU	Cisco	2RU w/Motherboard;1 CPU;RAID;Pwr Supp;NO Drives;NO Options	1
CIVS-CAB-16-AC	CIVS-CAB-16-AC	Cisco	CIVS C16 Power Cable North America	2
CIVS-HDD-1000	CIVS-HDD-1000	Cisco	1TB SATA Drive for CIVS-MSP	12
CIVS-MS-SW6.2	CIVS-MS-SW6.2	Cisco	CIVS-MS Media Server v6.2 Software License with Hardware	1
CIVS-PS-900	CIVS-PS-900	Cisco	Redundant 900W Power Supply for CIVS-MSP 2RU, 4RU	1
CIVS-VSM-SW4262	CIVS-VSM-SW4262	Cisco	CIVS-VSM Video Surveillance Manager v4.2/6.2 SW Mfg Image	1
CON-SNT-VSM2U	CON-SNT-VSM2U	Cisco	SMARTNET 8X5XNBD 2RU MSP Assembly	1
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	2
CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	2
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C3560-8PC-S	WS-C3560-8PC-S	Cisco	Catalyst 3560 Compact 8 10/100 PoE + 1 T/SFP; IP Base Image	20
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	20
CON-SNTP-WSC3568	CON-SNTP-WSC3568	Cisco	SMARTNET 24X7X4 Catalyst 3560 8 10/1	20
WS-C3560X-24P-S	WS-C3560X-24P-S	Cisco	Cisco Catalyst 3560X 24 Port PoE IP Base	6
C3KX-PWR-715WAC	C3KX-PWR-715WAC	Cisco	Cisco Catalyst 3K-X 715W AC Power Supply	6
C3KX-NM-1G	C3KX-NM-1G	Cisco	Cisco Catalyst 3K-X 1G Network Module option PID	6
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	6
CON-SNT-3560X2PS	CON-SNT-3560X2PS	Cisco	SMARTNET 8X5XNBD Catalyst 3560X 24 Port PoE IP Base	6
S356XVK9T-12253SE	S356XVK9T-12253SE	Cisco	CAT 3560X IOS UNIVERSAL WITH WEB BASED DEV MGR	6
SFP-GE-S=	SFP-GE-S=	Cisco	1000BASE-SX SFP (DOM)	12

WS-C4507R+E	WS-C4507R+E	Cisco	Cisco Catalyst 4500E 7 slot chassis for 48Gbps/slot	2
C4500E-IPB	C4500E-IPB	Cisco	Paper IP Base License	2
CAB-AC-2800W-TWLK	CAB-AC-2800W-TWLK	Cisco	U.S. Power Cord, Twist Lock, NEMA 6-20 Plug	4
CON-SNT-C4507R+E	CON-SNT-C4507R+E	Cisco	SMARTNET 8X5XNBD Catalyst4500E 7 slot chassis for 48Gbps	2
GLC-SX-MM=	GLC-SX-MM=	Cisco	GE SFP, LC connector SX transceiver	48
PWR-C45-2800ACV	PWR-C45-2800ACV	Cisco	Cisco Catalyst 4500 2800W AC Power Supply (Data and PoE)	2
PWR-C45-2800ACV/2	PWR-C45-2800ACV/2	Cisco	Cisco Catalyst 4500 2800W AC Power Supply (Data and PoE)	2
S45UK9-31-01XO	S45UK9-31-01XO	Cisco	CAT4500e SUP7e Universal Crypto Image	2
WS-X4448-GB-SFP	WS-X4448-GB-SFP	Cisco	Cisco Catalyst 4500 48-Port 1000Base-X (SFPs Optional)	2
WS-X45-SUP7-E	WS-X45-SUP7-E	Cisco	Cisco Catalyst 4500 E-Series Supervisor, 848Gbps	2
WS-X45-SUP7-E/2	WS-X45-SUP7-E/2	Cisco	Cisco Catalyst 4500 E-Series Supervisor, 848Gbps	2
WS-X4624-SFP-E	WS-X4624-SFP-E	Cisco	Cisco Catalyst 4500 E-Series 24-Port GE (SFP)	2
WS-X4748-RJ45V+E	WS-X4748-RJ45V+E	Cisco	Cisco Catalyst 4500E 48-Port PoE 802.3at 10/100/1000(RJ45)	2

Data Center, Internet Edge, DMZ

Name	Catalog Num	Vendor	Description	Qty
ASA5585-S60-2A-K9	ASA5585-S60-2A-K9	Cisco	Cisco ASA 5585-X Chas w/ SSP60,6 GE,4 SFP+,2 GE Mgt,2 AC,3DES/AES	2
ASA-SSP-60-INC	ASA-SSP-60-INC	Cisco	Cisco ASA 5585-X Security Services Processor-60 with 6GE, 4SFP+	2
ASA-VPN-CLNT-K9	ASA-VPN-CLNT-K9	Cisco	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	2
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	Cisco ASA 5500 Strong Encryption License (3DES/AES)	2
ASA5585-BLANK-F	ASA5585-BLANK-F	Cisco	Cisco ASA 5585-X Full Width Blank Slot Cover	2
ASA5585-BLANK-HD	ASA5585-BLANK-HD	Cisco	Cisco ASA 5585-X Hard Drive Blank Slot Cover	4

ASA5585-PWR-AC	ASA5585-PWR-AC	Cisco	Cisco ASA 5585-X AC Power Supply	4
ASA-ADV-END-SEC	ASA-ADV-END-SEC	Cisco	Cisco ASA 5500 Advanced Endpoint Assessment License for SSL VPN	2
ASA5500-SC-10	ASA5500-SC-10	Cisco	Cisco ASA 5500 10 Security Contexts License	2
ASA5500-SSL-1000	ASA5500-SSL-1000	Cisco	Cisco ASA 5500 SSL VPN 1000 Premium User License	2
CAB-US515P-C19-US	CAB-US515P-C19-US	Cisco	NEMA 5-15 to IEC-C19 13ft US	4
CON-SNT-A85S62K9	CON-SNT-A85S62K9	Cisco	SMARTNET 8X5XNBD ASA 5585-X Chas w/ SSP40,6 GE,4 SFP+,2 G	2
SF-ASA5585-8.2-K8	SF-ASA5585-8.2-K8	Cisco	Cisco ASA 5500 Series Software Version 8.2 for ASA 5585-X, DES	2
ASR1002-5G-SHA/K9	ASR1002-5G-SHA/K9	Cisco	Cisco ASR1002 Sec+HA Bundle w/ ESP-5G,AESK9,License,4GB DRAM	2
ASR1000-ESP5	ASR1000-ESP5	Cisco	Cisco ASR1K Embedded Services Processor,5Gbps,ASR1002 only	2
FLASR1-FPI-RTU	FLASR1-FPI-RTU	Cisco	Flex. Pack Insp. Right-To-Use Feat Lic,ASR1000 Series	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
FLASR1-IPSEC-RTU	FLASR1-IPSEC-RTU	Cisco	Encryption Right-To-Use Feature Lic for ASR1000 Series	2
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1002-PWR-AC	ASR1002-PWR-AC	Cisco	Cisco ASR1002 AC Power Supply	4
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	4
CON-SNTP-25GSHAK9	CON-SNTP-25GSHAK9	Cisco	SMARTNET 24X7X4 ASR1002 Sec+HA Bundle w/ESP-5G, AESK9	2
ASR1004-20G-HA/K9	ASR1004-20G-HA/K9	Cisco	Cisco ASR1004 HA Bundle w/ ESP-20G,RP1,SIP10,AESK9,License	2
ASR1000-ESP20	ASR1000-ESP20	Cisco	Cisco ASR1000 Embedded Services Processor, 20G	2
ASR1000-SPA	ASR1000-SPA	Cisco	SPA for ASR1000; No Physical Part; For Tracking Only	4
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
M-ASR1K-HDD-40GB	M-ASR1K-HDD-40GB	Cisco	Cisco ASR1000 RP1 40GB HDD	2
M-ASR1K-RP1-4GB	M-ASR1K-RP1-4GB	Cisco	Cisco ASR1000 RP1 4GB DRAM	2

SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1000-RP1-BUN	ASR1000-RP1-BUN	Cisco	Cisco ASR1000 Route Processor 1, 4GB DRAM,Bundle Component	2
ASR1000-SIP10	ASR1000-SIP10	Cisco	Cisco ASR1000 SPA Interface Processor 10	2
ASR1000-SIP10-BUN	ASR1000-SIP10-BUN	Cisco	Cisco ASR1000 SPA Interface Processor 10, Bundle Component	2
ASR1004-PWR-AC	ASR1004-PWR-AC	Cisco	Cisco ASR1004 AC Power Supply	4
CAB-AC15A-90L-US	CAB-AC15A-90L-US	Cisco	15A AC Pwr Cord, left-angle (United States) (bundle option)	4
CON-SNTP-420GHAK9	CON-SNTP-420GHAK9	Cisco	SMARTNET 24X7X4 ASR1004 Chassis 2 P/S	2
CON-SNTP-A1ESP20	CON-SNTP-A1ESP20	Cisco	SMARTNET 24X7X4 ASR1000 Embedded Svc Processor,20G,Crypt	2
CON-SNTP-ASRRP1B	CON-SNTP-ASRRP1B	Cisco	SMARTNET 24X7X4 Cisco ASR1000 Route Processor 1	2
CON-SNTP-ASRSIPB	CON-SNTP-ASRSIPB	Cisco	SMARTNET 24X7X4 Cisco ASR1000 SPA Interface Processor	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
SPA-1X10GE-L-V2	SPA-1X10GE-L-V2	Cisco	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter	4
XFP-10G-MM-SR	XFP-10G-MM-SR	Cisco	10GBASE-SR XFP Module	4
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
Ironport Bundle E-mail and Web	Ironport Bundle E-mail and Web	Cisco	Ironport A La Carte examples for Webn and E-mail	2
N5K-C5020P-NBF	N5K-C5020P-NBF	Cisco	Cisco Nexus 5020 NetApp OSM version, 2 PS	2
N5020-ACC-KIT	N5020-ACC-KIT	Cisco	Cisco Nexus 5020 Accessory Kit, Option	2
N5K-PAC-1200W	N5K-PAC-1200W	Cisco	Cisco Nexus 5020 PSU module, 100-240VAC 1200W	4
CAB-9K12A-NA	CAB-9K12A-NA	Cisco	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4

CON-SNTP-N5020	CON-SNTP-N5020	Cisco	SMARTNET 24X7X4 N5000 2RU Chassis no PS 5	2
N5000FMS1K9	N5000FMS1K9	Cisco	Cisco Nexus 5000 Fabric Manager Server License	2
N5K-M1600	N5K-M1600	Cisco	N5000 1000 Series Module 6port 10GE(req SFP+)	4
N5KUK9-421N2.1	N5KUK9-421N2.1	Cisco	Cisco Nexus 5000 Base OS Software Rel 4.2(1)N2(1)	2
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	16
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	64
WS-C3750X-24T-S	WS-C3750X-24T-S	Cisco	Cisco Catalyst 3750X 24 Port Data IP Base	6
C3KX-PWR-350WAC	C3KX-PWR-350WAC	Cisco	Cisco Catalyst 3K-X 350W AC Power Supply	6
S375XVK9T-12255SE	S375XVK9T-12255SE	Cisco	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	6
C3KX-PWR-350WAC/2	C3KX-PWR-350WAC/2	Cisco	Cisco Catalyst 3K-X 350W AC Secondary Power Supply	6
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	12
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	6
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	6
CON-SNTP-3750X2TS	CON-SNTP-3750X2TS	Cisco	SMARTNET 24X7X4 Catalyst 3750X 24 Port Data IP Base	6
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1
BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
SF-FWM-ASDM-6.1F	SF-FWM-ASDM-6.1F	Cisco	Device Manager for FWSM 4.0 for Catalyst 6500 and 7600	1
VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1

WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE-16G-LIC	ACE-16G-LIC	Cisco	ACE20 16Gbps License	1
ACE-SSL-05K-K9	ACE-SSL-05K-K9	Cisco	Application Control Engine SSL License, 5000 TPS	1
ACE-VIRT-020	ACE-VIRT-020	Cisco	Application Control Engine Virtualization 20 Contexts	1
ACE20-MOD-K9	ACE20-MOD-K9	Cisco	Application Control Engine 20 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4
CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1
CON-SNT-ACE20MOD	CON-SNT-ACE20MOD	Cisco	SMARTNET 8X5XNBD Application Control	1
CON-SNT-WS-FWM1K9	CON-SNT-WS-FWM1K9	Cisco	8x5xNBD Svc, Firewall blade for Catalyst 6500	1
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
SC-SVC-FWM-4.0-K9	SC-SVC-FWM-4.0-K9	Cisco	Firewall Module Software 4.0 for 6500 and 7600, 2 free VFW	1
SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SC6K-A23-ACE	SC6K-A23-ACE	Cisco	ACE Module Software A2(3)	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cisco Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1
WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2
WS-SVC-FWM-1-K9	WS-SVC-FWM-1-K9	Cisco	Firewall blade for 6500 and 7600, VFW License Separate	1
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K9	Cisco	600M IDSM-2 Mod for Cat	1
WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1

X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1
BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
SF-FWM-ASDM-6.1F	SF-FWM-ASDM-6.1F	Cisco	Device Manager for FWSM 4.0 for Catalyst 6500 and 7600	1
VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE-16G-LIC	ACE-16G-LIC	Cisco	ACE20 16Gbps License	1
ACE-SSL-05K-K9	ACE-SSL-05K-K9	Cisco	Application Control Engine SSL License, 5000 TPS	1
ACE-VIRT-020	ACE-VIRT-020	Cisco	Application Control Engine Virtualization 20 Contexts	1
ACE20-MOD-K9	ACE20-MOD-K9	Cisco	Application Control Engine 20 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4
CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1
CON-SNT-ACE20MOD	CON-SNT-ACE20MOD	Cisco	SMARTNET 8X5XNBD Application Control	1
CON-SNT-WS-FWM1K9	CON-SNT-WS-FWM1K9	Cisco	8x5xNBD Svc, Firewall blade for Catalyst 6500	1
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
SC-SVC-FWM-4.0-K9	SC-SVC-FWM-4.0-K9	Cisco	Firewall Module Software 4.0 for 6500 and 7600, 2 free VFW	1

SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SC6K-A23-ACE	SC6K-A23-ACE	Cisco	ACE Module Software A2(3)	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1
WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2
WS-SVC-FWM-1-K9	WS-SVC-FWM-1-K9	Cisco	Firewall blade for 6500 and 7600, VFW License Separate	1
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K9	Cisco	600M IDSM-2 Mod for Cat	1
WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18

Data Center—WAN Aggregation

Name	Catalog Num	Vendor	Description	Qty
ASA5540-AIP40-K9	ASA5540-AIP40-K9	Cisco	ASA 5540 Appliance w/ AIP-SSM-40, SW, HA, 4GE+1FE, 3DES/AES	4
ASA-AIP-40-INC-K9	ASA-AIP-40-INC-K9	Cisco	ASA 5500 AIP Security Services Module-40 included w/ bundles	4
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	4
ASA5540-VPN-PR	ASA5540-VPN-PR	Cisco	ASA 5540 VPN Premium 5000 IPsec User License (7.0 Only)	4
ASA-AC-E-5540	ASA-AC-E-5540	Cisco	AnyConnect Essentials VPN License - ASA 5540 (2500 Users)	4
ASA-AC-M-5540	ASA-AC-M-5540	Cisco	AnyConnect Mobile - ASA 5540 (req. Essentials or Premium)	4
ASA-VPN-CLNT-K9	ASA-VPN-CLNT-K9	Cisco	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	4
ASA-VPNS-1000	ASA-VPNS-1000	Cisco	Premium Shared VPN Server License - 1000 users	4

ASA5500-SC-5	ASA5500-SC-5	Cisco	Cisco ASA 5500 5 Security Contexts License	4
ASA5500-SSL-100	ASA5500-SSL-100	Cisco	Cisco ASA 5500 SSL VPN 100 Premium User License	4
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CON-SU3-AS4A40K9	CON-SU3-AS4A40K9	Cisco	IPS SVC, AR 24X7X4 ASA5540-AIP40-K9	4
SF-ASA-8.3-K8	SF-ASA-8.3-K8	Cisco	Cisco ASA 5500 Series Software v8.3	4
SF-ASA-AIP-7.0-K9	SF-ASA-AIP-7.0-K9	Cisco	Cisco ASA 5500 Series AIP Sofware 7.0 for Security Service Modules	4
ASR1002-5G-SHA/K9	ASR1002-5G-SHA/K9	Cisco	Cisco ASR1002 Sec+HA Bundle w/ ESP-5G,AESK9,License,4GB DRAM	4
ASR1000-ESP5	ASR1000-ESP5	Cisco	Cisco ASR1K Embedded Services Processor,5Gbps,ASR1002 only	4
FLASR1-FPI-RTU	FLASR1-FPI-RTU	Cisco	Flex. Pack Insp. Right-To-Use Feat Lic,ASR1000 Series	4
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	4
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	4
FLASR1-IPSEC-RTU	FLASR1-IPSEC-RTU	Cisco	Encryption Right-To-Use Feature Lic for ASR1000 Series	4
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	4
ASR1002-PWR-AC	ASR1002-PWR-AC	Cisco	Cisco ASR1002 AC Power Supply	8
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	8
CON-SNTP-25GSHAK9	CON-SNTP-25GSHAK9	Cisco	SMARTNET 24X7X4 ASR1002 Sec+HA Bundle w/ESP-5G, AESK9	4
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
IPS-4260-4GE-BP-K9	IPS-4260-4GE-BP-K9	Cisco	4260 Bundle with 4-Port Cu NIC	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2

CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CON-P2SP-4260-4G	CON-P2SP-4260-4G	Cisco	PM2, 24X7X4 IPS-4260-4GE-BP-K9	2
IPS-4260-PWR	IPS-4260-PWR	Cisco	Redundant power for 4260	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
IPS-SW-6.2	IPS-SW-6.2	Cisco	Cisco IPS Sensor software version 6.2	2
WS-C3750X-24T-S	WS-C3750X-24T-S	Cisco	Cisco Catalyst 3750X 24 Port Data IP Base	8
C3KX-PWR-350WAC	C3KX-PWR-350WAC	Cisco	Cisco Catalyst 3K-X 350W AC Power Supply	8
S375XVK9T-12255SE	S375XVK9T-12255SE	Cisco	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	8
C3KX-PWR-350WAC/2	C3KX-PWR-350WAC/2	Cisco	Cisco Catalyst 3K-X 350W AC Secondary Power Supply	8
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	16
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	8
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	8
CON-SNTP-3750X2TS	CON-SNTP-3750X2TS	Cisco	SMARTNET 24X7X4 Catalyst 3750X 24 Port Data IP Base	8

Data Center—Service

Name	Catalog Num	Vendor	Description	Qty
ASA5585-S60-2A-K9	ASA5585-S60-2A-K9	Cisco	ASA 5585-X Chas w/ SSP60,6 GE,4 SFP+,2 GE Mgt,2 AC,3DES/AES	2
ASA-SSP-60-INC	ASA-SSP-60-INC	Cisco	ASA 5585-X Security Services Processor-60 with 6GE, 4SFP+	2
ASA-VPN-CLNT-K9	ASA-VPN-CLNT-K9	Cisco	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	2
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	Cisco ASA 5500 Strong Encryption License (3DES/AES)	2
ASA5585-BLANK-F	ASA5585-BLANK-F	Cisco	Cisco ASA 5585-X Full Width Blank Slot Cover	2
ASA5585-BLANK-HD	ASA5585-BLANK-HD	Cisco	Cisco ASA 5585-X Hard Drive Blank Slot Cover	4

ASA5585-PWR-AC	ASA5585-PWR-AC	Cisco	Cisco ASA 5585-X AC Power Supply	4
ASA-ADV-END-SEC	ASA-ADV-END-SEC	Cisco	Cisco ASA 5500 Advanced Endpoint Assessment License for SSL VPN	2
ASA5500-SC-10	ASA5500-SC-10	Cisco	Cisco ASA 5500 10 Security Contexts License	2
CAB-US515P-C19-US	CAB-US515P-C19-US	Cisco	NEMA 5-15 to IEC-C19 13ft US	4
CON-SNT-A85S62K9	CON-SNT-A85S62K9	Cisco	SMARTNET 8X5XNBD ASA 5585-X Chas w/ SSP40,6 GE,4 SFP+,2 G	2
SF-ASA5585-8.2-K8	SF-ASA5585-8.2-K8	Cisco	Cisco ASA 5500 Series Software Version 8.2 for ASA 5585-X, DES	2
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
IPS4270-2X10GE-K9	IPS4270-2X10GE-K9	Cisco	IPS 4270-20 bundled with 2-port 10GE NIC	2
IPS-2X10GE-SR-INC	IPS-2X10GE-SR-INC	Cisco	2X10GE interface card included in 10GE 4270 bundle	2
CAB-US515P-C19-US	CAB-US515P-C19-US	Cisco	NEMA 5-15 to IEC-C19 13ft US	4
CON-P2ST-IPS42702	CON-P2ST-IPS42702	Cisco	PM2, 8X5XNBD IPS 4270-20 bundled	2
IPS-2SX-INT	IPS-2SX-INT	Cisco	2-port fiber interface for the 4260 and 4270	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
IPS-SW-7.0	IPS-SW-7.0	Cisco	Cisco IPS software version 7.0	2
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1
BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
SF-FWM-ASDM-6.1F	SF-FWM-ASDM-6.1F	Cisco	Device Manager for FWSM 4.0 for Catalyst 6500 and 7600	1

VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE-16G-LIC	ACE-16G-LIC	Cisco	ACE20 16Gbps License	1
ACE-SSL-05K-K9	ACE-SSL-05K-K9	Cisco	Application Control Engine SSL License, 5000 TPS	1
ACE-VIRT-020	ACE-VIRT-020	Cisco	Application Control Engine Virtualization 20 Contexts	1
ACE20-MOD-K9	ACE20-MOD-K9	Cisco	Application Control Engine 20 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4
CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1
CON-SNT-ACE20MOD	CON-SNT-ACE20MOD	Cisco	SMARTNET 8X5XNBD Application Control	1
CON-SNT-WS-FWM1K9	CON-SNT-WS-FWM1K9	Cisco	8x5xNBD Svc, Firewall blade for Catalyst 6500	1
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
SC-SVC-FWM-4.0-K9	SC-SVC-FWM-4.0-K9	Cisco	Firewall Module Software 4.0 for 6500 and 7600, 2 free VFW	1
SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SC6K-A23-ACE	SC6K-A23-ACE	Cisco	ACE Module Software A2(3)	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1
WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2

WS-SVC-FWM-1-K9	WS-SVC-FWM-1-K9	Cisco	Firewall blade for 6500 and 7600, VFW License Separate	1
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K9	Cisco	600M IDSM-2 Mod for Cat	1
WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1
BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
SF-FWM-ASDM-6.1F	SF-FWM-ASDM-6.1F	Cisco	Device Manager for FWSM 4.0 for Catalyst 6500 and 7600	1
VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE-16G-LIC	ACE-16G-LIC	Cisco	ACE20 16Gbps License	1
ACE-SSL-05K-K9	ACE-SSL-05K-K9	Cisco	Application Control Engine SSL License, 5000 TPS	1
ACE-VIRT-020	ACE-VIRT-020	Cisco	Application Control Engine Virtualization 20 Contexts	1
ACE20-MOD-K9	ACE20-MOD-K9	Cisco	Application Control Engine 20 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4
CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1

CON-SNT-ACE20MOD	CON-SNT-ACE20MOD	Cisco	SMARTNET 8X5XNBD Application Control	1
CON-SNT-WS-FWM1K9	CON-SNT-WS-FWM1K9	Cisco	8x5xNBD Svc, Firewall blade for Catalyst 6500	1
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
SC-SVC-FWM-4.0-K9	SC-SVC-FWM-4.0-K9	Cisco	Firewall Module Software 4.0 for 6500 and 7600, 2 free VFW	1
SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SC6K-A23-ACE	SC6K-A23-ACE	Cisco	ACE Module Software A2(3)	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1
WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2
WS-SVC-FWM-1-K9	WS-SVC-FWM-1-K9	Cisco	Firewall blade for 6500 and 7600, VFW License Separate	1
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K9	Cisco	600M IDSM-2 Mod for Cat	1
WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18

Data Center—Secure Storage

Name	Catalog Num	Vendor	Description	Qty
DS-C9509-2AK9	DS-C9509-2AK9	Cisco	MDS 9509 Base Config: Chassis, 2 Sup-2A, 2 3K AC PS	2
CAB-9K16A-US2	CAB-9K16A-US2	Cisco	Power Cord 250VAC 16A, US/Japan, Src Plug NEMA L6-20	4
CON-SNT-4848K	CON-SNT-4848K	Cisco	SMARTNET 8X5XNBD Host Optimized 8G FC	4
CON-SNT-9304K	CON-SNT-9304K	Cisco	SMARTNET 8X5XNBD MDS 9000 18-port FC and 4-port GE Module	2

CON-SNT-C9509U	CON-SNT-C9509U	Cisco	SMARTNET 8X5XNBD MDS 9509 Base Config: Chassis, 2 Sup-2A	2
DS-9509-KIT-EMC	DS-9509-KIT-EMC	Cisco	MDS 9509 Accessory Kit for EMC	2
DS-SFP-FC4G-SW	DS-SFP-FC4G-SW	Cisco	4 Gbps Fibre Channel-SW SFP, LC	36
DS-SFP-FC8G-SW	DS-SFP-FC8G-SW	Cisco	8 Gbps Fibre Channel SW SFP+, LC	192
DS-X9248-48K9	DS-X9248-48K9	Cisco	4/44-Port Host-Optimized 8-Gbps FC Module	4
DS-X9304-18K9	DS-X9304-18K9	Cisco	MDS 9000 18-port FC and 4-port GE Module	2
M9500ENT1K9	M9500ENT1K9	Cisco	Enterprise package license for 1 MDS9500 switch	2
M9500SSE1K9	M9500SSE1K9	Cisco	Storage Services Enabler: 1 ASM on 1 MDS9500	2
M95IOA184	M95IOA184	Cisco	Cisco I/O Accelerator License for MSM-18/4 on MDS 9500	2
M95S2K9-5.0.4	M95S2K9-5.0.4	Cisco	MDS 9500 Supervisor/Fabric-2, NX-OS Software Release 5.0(4)	2
SSI-M9K9-504	SSI-M9K9-504	Cisco	MDS SSI Image 5.0(4)	2

Data Center—Extranet Edge

Name	Catalog Num	Vendor	Description	Qty
ASA5585-S60-2A-K9	ASA5585-S60-2A-K9	Cisco	Cisco ASA 5585-X Chas w/ SSP60,6 GE,4 SFP+,2 GE Mgt,2 AC,3DES/AES	2
ASA-SSP-60-INC	ASA-SSP-60-INC	Cisco	Cisco ASA 5585-X Security Services Processor-60 with 6GE, 4SFP+	2
ASA-VPN-CLNT-K9	ASA-VPN-CLNT-K9	Cisco	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	2
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	Cisco ASA 5500 Strong Encryption License (3DES/AES)	2
ASA5585-BLANK-F	ASA5585-BLANK-F	Cisco	Cisco ASA 5585-X Full Width Blank Slot Cover	2
ASA5585-BLANK-HD	ASA5585-BLANK-HD	Cisco	Cisco ASA 5585-X Hard Drive Blank Slot Cover	4
ASA5585-PWR-AC	ASA5585-PWR-AC	Cisco	Cisco ASA 5585-X AC Power Supply	4
ASA-ADV-END-SEC	ASA-ADV-END-SEC	Cisco	Cisco ASA 5500 Advanced Endpoint Assessment License for SSL VPN	2
ASA5500-SC-10	ASA5500-SC-10	Cisco	Cisco ASA 5500 10 Security Contexts License	2

ASA5500-SSL-1000	ASA5500-SSL-1000	Cisco	Cisco ASA 5500 SSL VPN 1000 Premium User License	2
CAB-US515P-C19-US	CAB-US515P-C19-US	Cisco	NEMA 5-15 to IEC-C19 13ft US	4
CON-SNT-A85S62K9	CON-SNT-A85S62K9	Cisco	SMARTNET 8X5XNBD ASA 5585-X Chas w/ SSP40,6 GE,4 SFP+,2 G	2
SF-ASA5585-8.2-K8	SF-ASA5585-8.2-K8	Cisco	Cisco ASA 5500 Series Software Version 8.2 for ASA 5585-X, DES	2
ASR1002-5G-SHA/K9	ASR1002-5G-SHA/K9	Cisco	Cisco ASR1002 Sec+HA Bundle w/ ESP-5G,AESK9,License,4GB DRAM	2
ASR1000-ESP5	ASR1000-ESP5	Cisco	Cisco ASR1K Embedded Services Processor,5Gbps,ASR1002 only	2
FLASR1-FPI-RTU	FLASR1-FPI-RTU	Cisco	Flex. Pack Insp. Right-To-Use Feat Lic,ASR1000 Series	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
FLASR1-IPSEC-RTU	FLASR1-IPSEC-RTU	Cisco	Encryption Right-To-Use Feature Lic for ASR1000 Series	2
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1002-PWR-AC	ASR1002-PWR-AC	Cisco	Cisco ASR1002 AC Power Supply	4
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	4
CON-SNTP-25GSHAK9	CON-SNTP-25GSHAK9	Cisco	SMARTNET 24X7X4 ASR1002 Sec+HA Bundle w/ESP-5G, AESK9	2
ASR1004-20G-HA/K9	ASR1004-20G-HA/K9	Cisco	ASR1004 HA Bundle w/ ESP-20G,RP1,SIP10,AESK9,License	2
ASR1000-ESP20	ASR1000-ESP20	Cisco	Cisco ASR1000 Embedded Services Processor, 20G	2
ASR1000-SPA	ASR1000-SPA	Cisco	SPA for ASR1000; No Physical Part; For Tracking Only	4
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
M-ASR1K-HDD-40GB	M-ASR1K-HDD-40GB	Cisco	Cisco ASR1000 RP1 40GB HDD	2
M-ASR1K-RP1-4GB	M-ASR1K-RP1-4GB	Cisco	Cisco ASR1000 RP1 4GB DRAM	2
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1000-RP1-BUN	ASR1000-RP1-BUN	Cisco	Cisco ASR1000 Route Processor 1, 4GB DRAM,Bundle Component	2
ASR1000-SIP10	ASR1000-SIP10	Cisco	Cisco ASR1000 SPA Interface Processor 10	2

ASR1000-SIP10-BUN	ASR1000-SIP10-BUN	Cisco	Cisco ASR1000 SPA Interface Processor 10, Bundle Component	2
ASR1004-PWR-AC	ASR1004-PWR-AC	Cisco	Cisco ASR1004 AC Power Supply	4
CAB-AC15A-90L-US	CAB-AC15A-90L-US	Cisco	15A AC Pwr Cord, left-angle (United States) (bundle option)	4
CON-SNTP-420GHAK9	CON-SNTP-420GHAK 9	Cisco	SMARTNET 24X7X4 ASR1004 Chassis 2 P/S	2
CON-SNTP-A1ESP20	CON-SNTP-A1ESP20	Cisco	SMARTNET 24X7X4 ASR1000 Embedded Svc Processor,20G,Crypt	2
CON-SNTP-ASRRP1B	CON-SNTP-ASRRP1B	Cisco	SMARTNET 24X7X4 Cisco ASR1000 Route Processor 1	2
CON-SNTP-ASRSIPB	CON-SNTP-ASRSIPB	Cisco	SMARTNET 24X7X4 Cisco ASR1000 SPA Interface Processor	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
SPA-1X10GE-L-V2	SPA-1X10GE-L-V2	Cisco	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter	4
XFP-10G-MM-SR	XFP-10G-MM-SR	Cisco	10GBASE-SR XFP Module	4
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
IPS-4260-4GE-BP-K9	IPS-4260-4GE-BP-K9	Cisco	4260 Bundle with 4-Port Cu NIC	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CON-P2SP-4260-4G	CON-P2SP-4260-4G	Cisco	PM2, 24X7X4 IPS-4260-4GE-BP-K9	2
IPS-4260-PWR	IPS-4260-PWR	Cisco	Redundant power for 4260	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
IPS-SW-6.2	IPS-SW-6.2	Cisco	Cisco IPS Sensor software version 6.2	2
N5K-C5020P-NBF	N5K-C5020P-NBF	Cisco	Cisco Nexus 5020 NetApp OSM version, 2 PS	2

N5020-ACC-KIT	N5020-ACC-KIT	Cisco	Nexus 5020 Accessory Kit, Option	2
N5K-PAC-1200W	N5K-PAC-1200W	Cisco	Nexus 5020 PSU module, 100-240VAC 1200W	4
CAB-9K12A-NA	CAB-9K12A-NA	Cisco	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4
CON-SNTP-N5020	CON-SNTP-N5020	Cisco	SMARTNET 24X7X4 N5000 2RU Chassis no PS 5	2
N5000FMS1K9	N5000FMS1K9	Cisco	Nexus 5000 Fabric Manager Server License	2
N5K-M1600	N5K-M1600	Cisco	N5000 1000 Series Module 6port 10GE(req SFP+)	4
N5KUK9-421N2.1	N5KUK9-421N2.1	Cisco	Nexus 5000 Base OS Software Rel 4.2(1)N2(1)	2
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	16
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	64
WS-C3750X-24T-S	WS-C3750X-24T-S	Cisco	Cisco Catalyst 3750X 24 Port Data IP Base	8
C3KX-PWR-350WAC	C3KX-PWR-350WAC	Cisco	Cisco Catalyst 3K-X 350W AC Power Supply	8
S375XVK9T-12255SE	S375XVK9T-12255SE	Cisco	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	8
C3KX-PWR-350WAC/2	C3KX-PWR-350WAC/2	Cisco	Cisco Catalyst 3K-X 350W AC Secondary Power Supply	8
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	16
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	8
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	8
CON-SNTP-3750X2TS	CON-SNTP-3750X2TS	Cisco	SMARTNET 24X7X4 Catalyst 3750X 24 Port Data IP Base	8

Data Center—Physical Security

Name	Catalog Num	Vendor	Description	Qty
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	8
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	8
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	8

CIAC-PAME-1125-K9	CIAC-PAME-1125-K9	Cisco	Cisco Physical Access Manager Appliance	4
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CIAC-SW-LNX-1.0-K9	CIAC-SW-LNX-1.0-K9	Cisco	Cisco PAM Appliance Software Version 1.0	4
CON-SNT-PAM1125	CON-SNT-PAM1125	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	4
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	4
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	4
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	4
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	4
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	4
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	4
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	4
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	4
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	4

CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	4
CIVS-MSP-4RU	CIVS-MSP-4RU	Cisco	4RU w/Motherboard;1 CPU;RAID;Pwr Suppl;NO Drives;NO Options	2
CIVS-CAB-16-AC	CIVS-CAB-16-AC	Cisco	CIVS C16 Power Cable North America	4
CIVS-FC-1P	CIVS-FC-1P	Cisco	1 Port FibreChannel Card for CIVS-MSP	2
CIVS-HDD-1000	CIVS-HDD-1000	Cisco	1TB SATA Drive for CIVS-MSP	48
CIVS-MS-SW6.2	CIVS-MS-SW6.2	Cisco	CIVS-MS Media Server v6.2 Software License with Hardware	2
CIVS-PS-900	CIVS-PS-900	Cisco	Redundant 900W Power Supply for CIVS-MSP 2RU, 4RU	2
CIVS-VSM-SW4262	CIVS-VSM-SW4262	Cisco	CIVS-VSM Video Surveillance Manager v4.2/6.2 SW Mfg Image	2
CON-SNT-VSM4U	CON-SNT-VSM4U	Cisco	SMARTNET 8X5XNBD 4RU MSP Assembly	2
CIVS-SS-4U-42000	CIVS-SS-4U-42000	Cisco	Cisco VS 4U Storage System with 42x1000GB drives	4
CON-SNT-VSS442K	CON-SNT-VSS442K	Cisco	SMARTNET 8X5XNBD CIVS-SS-4U-42000	4
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	10
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1

Data Center—Wireless Systems

Name	Catalog Num	Vendor	Description	Qty
AIR-CT5508-500-2PK	AIR-CT5508-500-2PK	Cisco	2x AIR-CT5508-500-K9	2
AIR-PWR-CORD-NA	AIR-PWR-CORD-NA	Cisco	AIR Line Cord North America	4
LIC-CT5508-500	LIC-CT5508-500	Cisco	500 AP Base license	4
LIC-CT5508-BASE	LIC-CT5508-BASE	Cisco	Base Software License	4
SWC5500K9-70	SWC5500K9-70	Cisco	Cisco Unified Wireless Controller SW Release 7.0	4
AIR-CT5508-500-K9Z	AIR-CT5508-500-K9Z	Cisco	5508 Series Controller for up to 500 APs	4

CON-SNTP-AIRC552P	CON-SNTP-AIRC552P	Cisco	SMARTNET 24X7X4 Two 5508 Series Controller for up to 500	2
AIR-MSE-3355-K9	AIR-MSE-3355-K9	Cisco	MSE 3355 Hardware SKU	2
AIR-MSE-PAK	AIR-MSE-PAK	Cisco	Mobility Services Configurable PAK	2
AIR-PWR-CORD-NA	AIR-PWR-CORD-NA	Cisco	AIR Line Cord North America	2
AIR-WIPS-AP-2000	AIR-WIPS-AP-2000	Cisco	Cisco wIPS License, Supporting Cisco 2000 Monitor Mode APs	2
SWMSE3355K9-70	SWMSE3355K9-70	Cisco	Cisco 3355 Series Mobility Services Engine SW Release 7.0	2
WCS-CD-K9	WCS-CD-K9	Cisco	CD With Windows And Linux. No License.	4
WCS-ENT-PLUS-K9	WCS-ENT-PLUS-K9	Cisco	Family SKU for WCS Enterprise PLUS License Products	1
CON-SAU-WENTK9	CON-SAU-WENTK9	Cisco	SW APP SUPP + UPGR Family SKU for WCS E	1
WCS-ENT-PLUS-10000	WCS-ENT-PLUS-10000	Cisco	Cisco WCS Enterprise PLUS License for 10,000 APs, Win/Linux	1

Data Center—Management

Name	Catalog Num	Vendor	Description	Qty
CSACS-1121-K9	CSACS-1121-K9	Cisco	ACS 1121 Appliance With 5.x SW And Base license	2
CSACS-5-BASE-LIC	CSACS-5-BASE-LIC	Cisco	Cisco Secure ACS 5 Base License	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	2
CON-SNTP-SACS1121	CON-SNTP-SACS1121	Cisco	SMARTNET 24X7X4 ACS 1121 Appliance With 5.1	2
CSACS-5-ADV-LIC	CSACS-5-ADV-LIC	Cisco	ACS 5 Security Group Access System License	2
CSACS-5.2-SW-K9	CSACS-5.2-SW-K9	Cisco	Config Option: ACS 5.2 Software Loaded On 1121	2
CSMPR-LIC-1000	CSMPR-LIC-1000	Cisco	Cisco Security Manager Pro - Incremental 1000 Device License	1
CON-P2S-CSMPRI1K	CON-P2S-CSMPRI1K	Cisco	PM2, SAS CSM Ent Pro -1K incr. dev license	1
CSMPR50-4.0-K9	CSMPR50-4.0-K9	Cisco	Cisco Security Manager 4.0 Professional w/ 50 Device License	1

CSMPR50-PAK4	CSMPR50-PAK4	Cisco	CS Mgr Enterprise Pro 50 - Secondary PAK	1
CON-CSSPS-CSMPR504	CON-CSSPS-CSMPR504	Cisco	SHARED SUPP SAS CS Mgr 4.0 Enterprise Pro 50 DeviceBase	1
CSMPR50-U-4.0-K9	CSMPR50-U-4.0-K9	Cisco	Cisco Security Manager 3.x to 4.0 Upgrade - PRO-50 License	1
CSMPR50-PAK4	CSMPR50-PAK4	Cisco	CS Mgr Enterprise Pro 50 - Secondary PAK	1
NAC3355-3500-K9	NAC3355-3500-K9	Cisco	NAC Appliance 3355 Server -max 3500 users	4
NAC3355-95-CAVACC	NAC3355-95-CAVACC	Cisco	NAC Appliance 3355-95 Cavium Accelerator	4
NAC3355-SVR	NAC3355-SVR	Cisco	NAC Appliance 3355 Server Hardware	4
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	8
CON-SNT-NAC535M	CON-SNT-NAC535M	Cisco	SMARTNET 8X5XNBD NAC3355-3500-K9	4
NAC-SVR-48-K9	NAC-SVR-48-K9	Cisco	NAC Appliance Server Release 4.8	4
NACMGR-M-STD-K9	NACMGR-M-STD-K9	Cisco	Cisco NAC Standard Manager for 20 servers	2
NAC3355	NAC3355	Cisco	NAC Appliance 3355 Manager Hardware	2
NAC3355-95-CAVACC	NAC3355-95-CAVACC	Cisco	NAC Appliance 3355-95 Cavium Accelerator	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CON-SNT-NAMSTDK9	CON-SNT-NAMSTDK9	Cisco	SMARTNET 8X5XNBD NACMGR-M-STD-K9	2
SPESMA-VC-BASE	SPESMA-VC-BASE	Cisco	EMC VoyenceControl Base	1
SP-PRODUCTS-TERMS	SP-PRODUCTS-TERMS	Cisco	Buyer Acceptance of SolutionsPlus Terms and Conditions	1
SPESMA-VC-LIC	SPESMA-VC-LIC	Cisco	EMC VoyenceControl License Card	1
SPESMA-VCMD-P	SPESMA-VCMD-P	Cisco	EMC VoyenceControl Prod Lic (RTU Lic per NOC/Data Ctr)	1
SPESMA-VCMD1-03	SPESMA-VCMD1-03	Cisco	EMC VoyenceControl Managed Tier 1 Device License: 1001-1500	1,200
SPESMA-VCMD2-03	SPESMA-VCMD2-03	Cisco	EMC VoyenceControl Managed Tier 2 Device License: 1001-1500	1,200
SPESMA-VCMD3-03	SPESMA-VCMD3-03	Cisco	EMC VoyenceControl Managed Tier 3 Device License: 1001-1500	1,200
SPESMA-VCO-LIC	SPESMA-VCO-LIC	Cisco	EMC Voyence PCI Advisor License Card	1

SPESMA-VCO-NA02	SPESMA-VCO-NA02	Cisco	EMC Voyence Network Advisor - Less Than 10,000 Devices	1
SPESMA-VCO-PCI	SPESMA-VCO-PCI	Cisco	EMC Voyence PCI Advisor	1

Data Center—Access, Aggregation

Name	Catalog Num	Vendor	Description	Qty
L-VLVSG-VNMC=	L-VLVSG-VNMC=	Cisco	Virtual Network Mgmt Center Base License for VSG eDelivery	1
CON-CSSPU-LVLVSG	CON-CSSPU-LVLVSG	Cisco	SHARED SUPP SAU Virtual Network Mgmt Center Base for VSG	1
CON-SAU-LVLVSG	CON-SAU-LVLVSG	Cisco	SW APP SUPP + UPGR Virtual Network Mgmt Center Base for VSG	1
L-VLVSG-VNMC-P1	L-VLVSG-VNMC-P1	Cisco	VSG and VNMC eDelivery CPU License Promo 1 Qty 32	32
N1K-C1010	N1K-C1010	Cisco	Cisco Nexus 1010 Virtual Services Appliance	1
A01-X0105	A01-X0105	Cisco	2.66GHz Xeon X5650 95W CPU/12MB cache/DDR3 1333MHz	2
CAB-C13-C14-JMPR	CAB-C13-C14-JMPR	Cisco	Recessed receptical AC power cord 27	1
N01-M304GB1	N01-M304GB1	Cisco	4GB DDR3-1333MHz RDIMM/PC3-10600/dual rank 1Gb DRAMs	4
N1K-VLCPU-32	N1K-VLCPU-32	Cisco	Nexus 1000V for Nexus 1010 Paper CPU License Qty 32	1
N2XX-ABPCI03	N2XX-ABPCI03	Cisco	Broadcom 5709 Quad Port 10/100/1Gb NIC w/TOE iSCSI	1
R200-BBLKD	R200-BBLKD	Cisco	HDD slot blanking panel for UCS C200 M1 Rack Servers	2
R200-BHTS1	R200-BHTS1	Cisco	CPU heat sink for UCS C200 M1 Rack Server	2
R200-D500GCSATA03	R200-D500GCSATA03	Cisco	Gen 2 500GB SATA 7.2K RPM 3.5in HDD/hot plug/C200 drive sled	2
R200-PCIBLKF1	R200-PCIBLKF1	Cisco	PCIe Full Height blanking panel for UCS C-Series Rack Server	1
R200-SASCBL-001	R200-SASCBL-001	Cisco	Internal SAS Cable for a base UCS C200 M1 Server	1
R2X0-ML002	R2X0-ML002	Cisco	LSI 1064E (4-port SAS 3.0G RAID 0, 1, 1E) Mezz Card	1
R2X0-PSU2-650W-SB	R2X0-PSU2-650W-SB	Cisco	650W power supply, w/added 5A Standby for UCS C200 or C210	1

R2XX-CMAG3-1032	R2XX-CMAG3-1032	Cisco	Cable Mgmt Arm for R2XX-G31032RAIL for C200/C210	1
R2XX-G31032RAIL	R2XX-G31032RAIL	Cisco	G3 shorter stronger Rail Kit for UCS 200, 210 Rack Servers	1
R2XX-PSUBLKP	R2XX-PSUBLKP	Cisco	Power supply unit blnking pnl for UCS 200 M1 or 210 M1	1
R2XX-RAID1	R2XX-RAID1	Cisco	Enable RAID 1 Setting	1
CAB-N5K6A-NA	CAB-N5K6A-NA	Cisco	Power Cord, 200/240V 6A North America	1
N1K-VLCPU-32=	N1K-VLCPU-32=	Cisco	Nexus 1000V Paper CPU License Qty 32 (1YR Min Service)	1
N1K-VLCPU-01	N1K-VLCPU-01	Cisco	Nexus 1000V Paper CPU License Qty 1	32
N5K-C5020P-NBF	N5K-C5020P-NBF	Cisco	Nexus 5020 NetApp OSM version, 2 PS	2
N5020-ACC-KIT	N5020-ACC-KIT	Cisco	Nexus 5020 Accessory Kit, Option	2
N5K-PAC-1200W	N5K-PAC-1200W	Cisco	Nexus 5020 PSU module, 100-240VAC 1200W	4
CAB-9K12A-NA	CAB-9K12A-NA	Cisco	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4
CON-SNTP-N5020	CON-SNTP-N5020	Cisco	SMARTNET 24X7X4 N5000 2RU Chassis no PS 5	2
N5000FMS1K9	N5000FMS1K9	Cisco	Nexus 5000 Fabric Manager Server License	2
N5K-M1600	N5K-M1600	Cisco	N5000 1000 Series Module 6port 10GE(req SFP+)	4
N5KUK9-421N2.1	N5KUK9-421N2.1	Cisco	Nexus 5000 Base OS Software Rel 4.2(1)N2(1)	2
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	16
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	64
N7K-C7010-BUN-R	N7K-C7010-BUN-R	Cisco	Nexus 7010 Bundle (Chassis,(2)SUP1,(3)FAB1,(3)AC-6KW PSU)	2
N7K-AC-6.0KW	N7K-AC-6.0KW	Cisco	Nexus 7000 - 6.0KW AC Power Supply Module	6
N7K-C7010-FAB1-BUN	N7K-C7010-FAB1-BUN	Cisco	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module	6
N7K-SUP1-BUN	N7K-SUP1-BUN	Cisco	Nexus 7000 - Supervisor 1, Includes External 8GB Flash	4
CAB-AC-2500W-US1	CAB-AC-2500W-US1	Cisco	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	12
CON-SNTP-C701BR	CON-SNTP-C701BR	Cisco	SMARTNET 24X7X4 Nexus 7010 Bundle	2

N7K-CPF-2GB	N7K-CPF-2GB	Cisco	Nexus Compact Flash Memory 2GB (Expansion Flash - Slot 0)	4
N7K-M132XP-12	N7K-M132XP-12	Cisco	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)	6
N7K-M148GT-11	N7K-M148GT-11	Cisco	Nexus 7000 - 48 Port 10/100/1000, RJ-45	2
N7KS1K9-50	N7KS1K9-50	Cisco	Cisco NX-OS Release 5.0	2
SFP-10G-SR	SFP-10G-SR	Cisco	10GBASE-SR SFP Module	34
WS-C4948-10GE-S	WS-C4948-10GE-S	Cisco	Catalyst 4948, IPB s/w, 48*10/100/1000+2*10GE(X2), 1 AC p/s	2
PWR-C49-300AC	PWR-C49-300AC	Cisco	Catalyst 4948 300-Watt AC Power Supply	2
S49IPB-12253SG	S49IPB-12253SG	Cisco	Cisco CAT4900 IOS IP BASE W/O CRYPTO	2
CAB-US515-C15-US	CAB-US515-C15-US	Cisco	NEMA 5-15 to IEC-C15 8ft US	2
CON-SNT-C4948GES	CON-SNT-C4948GES	Cisco	SMARTNET 8X5XNBD 4948, IPB s/w 4810/100/1K 2 10GE	2
X2-10GB-SR=	X2-10GB-SR=	Cisco	10GBASE-SR X2 Module	4

Data Center—UCS

Name	Catalog Num	Vendor	Description	Qty
N20-Z0001	N20-Z0001	Cisco	Cisco Unified Computing System	1
N1K-VLEM-UCS-1	N1K-VLEM-UCS-1	Cisco	Nexus 1000V License PAK For 1 Virtual Ethernet Module On UCS	32
VMW-VS-ENTP-1A	VMW-VS-ENTP-1A	Cisco	VMware vSphere Enterprise Plus (1 CPU), 1yr support required	32
A01-X0100	A01-X0100	Cisco	3.33GHz Xeon X5680 130W CPU/12MB cache/DDR3 1333MHz	64
A03-D146GC2	A03-D146GC2	Cisco	146GB 6Gb SAS 15K RPM SFF HDD/hot plug/drive sled mounted	64
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	16
CAB-N5K6A-NA	CAB-N5K6A-NA	Cisco	Power Cord, 200/240V 6A North America	4
CON-ISV1-VCS1A	CON-ISV1-VCS1A	Cisco	ISV 24X7 VMware vCenter Server Std 1 Yr RQD	32
CON-ISV1-VLEMUCS	CON-ISV1-VLEMUCS	Cisco	ISV 24X7 Nexus 1000V License PAK For 1 Virtual Et	64

CON-ISV1-VSENTP1A	CON-ISV1-VSENTP1A	Cisco	ISV 24X7 VMware vSphere EntPlus1CPU 1Yr RQD	32
CON-ISV1-VSENTP3A	CON-ISV1-VSENTP3A	Cisco	ISV 24X7 VMware vSphere EntPlus1CPU 3Yr RQD	32
CON-UCS1-1E0440	CON-UCS1-1E0440	Cisco	UC SUPPORT 8X5XNBD 4PT 10GE/4PT 4Gb FC/ExpanMod 6100Series	2
CON-UCS1-1S6200	CON-UCS1-1S6200	Cisco	UC SUPPORT 8X5XNBD 6140XP 40PT Fabric Interconnect	2
CON-UCS1-2C6508	CON-UCS1-2C6508	Cisco	UC SUPPORT 8X5XNBD 5108 Blade Server Chassis	4
CON-UCS1-2Z0001	CON-UCS1-2Z0001	Cisco	UC SUPPORT 8X5XNBD Cisco Unified Computing System	1
CON-UCS1-B66251	CON-UCS1-B66251	Cisco	UC SUPPORT 8X5XNBD UCSB200 M2 Blade Svr w/o CPU Mem HDD Mez	32
DS-SFP-FC4G-SW	DS-SFP-FC4G-SW	Cisco	4 Gbps Fibre Channel-SW SFP, LC	32
N01-M308GB2-L	N01-M308GB2-L	Cisco	8GB DDR3-1333MHz RDIMM/PC3-10600/dual rank/Low Voltage	384
N01-UAC1	N01-UAC1	Cisco	Single phase AC power module for UCS 5108	4
N10-E0440	N10-E0440	Cisco	4-port 10 GE/4-port 4Gb FC/Expansion module/UCS 6100 Series	2
N10-L001	N10-L001	Cisco	UCS 6100 Series Fabric Interconnect 1 10GE port license	32
N10-MGT005	N10-MGT005	Cisco	UCS Manager v1.3	2
N10-PAC2-750W	N10-PAC2-750W	Cisco	750W power supply unit for UCS 6140XP/100-240VAC	4
N10-S6200	N10-S6200	Cisco	UCS 6140XP 40-port Fabric Interconnect/0 PSU/5 fans/no SFP+	2
N10-SACCB	N10-SACCB	Cisco	Accessory kit for UCS 6140XP Fabric Interconnect	2
N10-SBLKE	N10-SBLKE	Cisco	Expansion module slot blanking panel for UCS 6100 Series	2
N1K-CSK9-UCS-404	N1K-CSK9-UCS-404	Cisco	Nexus 1000V VSM Virtual Appliance Software On UCS	32
N1K-VLEM-UCS-1	N1K-VLEM-UCS-1	Cisco	Nexus 1000V License PAK For 1 Virtual Ethernet Module On UCS	32
N20-AC0002	N20-AC0002	Cisco	UCS M81KR Virtual Interface Card/PCIe/2-port 10Gb	32
N20-B6625-1	N20-B6625-1	Cisco	UCS B200 M2 Blade Server w/o CPU, memory, HDD, mezzanine	32
N20-BHTS1	N20-BHTS1	Cisco	CPU heat sink for UCS B200 Blade Server	64

N20-C6508	N20-C6508	Cisco	UCS 5108 Blade Server Chassis/0 PSU/8 fans/0 fabric extender	4
N20-FAN5	N20-FAN5	Cisco	Fan module for UCS 5108	32
N20-FW005	N20-FW005	Cisco	UCS 5108 Blade Server Chassis FW package	4
N20-I6584	N20-I6584	Cisco	UCS 2104XP Fabric Extender/4 external 10Gb ports	8
N20-PAC5-2500W	N20-PAC5-2500W	Cisco	2500W power supply unit for UCS 5108	16
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	32
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	96
UCS-VMW-N1K-BUN	UCS-VMW-N1K-BUN	Cisco	Bundle of VMware Ent Plus and Nexus 1K License	32
VMW-VCS-1A	VMW-VCS-1A	Cisco	VMware vCenter Server Standard, 1yr support required	32
VMW-VS-ENTP-3A	VMW-VS-ENTP-3A	Cisco	VMware vSphere Enterprise Plus (1 CPU), 3yr support required	32

Data Center—Core

Name	Catalog Num	Vendor	Description	Qty
N7K-C7010-BUN-R	N7K-C7010-BUN-R	Cisco	Nexus 7010 Bundle (Chassis,(2)SUP1,(3)FAB1,(3)AC-6KW PSU)	1
N7K-AC-6.0KW	N7K-AC-6.0KW	Cisco	Nexus 7000 - 6.0KW AC Power Supply Module	3
N7K-C7010-FAB1-BUN	N7K-C7010-FAB1-BUN	Cisco	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module	3
N7K-SUP1-BUN	N7K-SUP1-BUN	Cisco	Nexus 7000 - Supervisor 1, Includes External 8GB Flash	2
CAB-AC-2500W-US1	CAB-AC-2500W-US1	Cisco	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	6
CON-SNTP-C701BR	CON-SNTP-C701BR	Cisco	SMARTNET 24X7X4 Nexus 7010 Bundle	1
N7K-M132XP-12	N7K-M132XP-12	Cisco	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)	3
N7K-M148GT-11	N7K-M148GT-11	Cisco	Nexus 7000 - 48 Port 10/100/1000, RJ-45	1
N7KS1K9-50	N7KS1K9-50	Cisco	Cisco NX-OS Release 5.0	1

N7K-C7010-BUN-R	N7K-C7010-BUN-R	Cisco	Nexus 7010 Bundle (Chassis,(2)SUP1,(3)FAB1,(3)AC-6KW PSU)	1
N7K-AC-6.0KW	N7K-AC-6.0KW	Cisco	Nexus 7000 - 6.0KW AC Power Supply Module	3
N7K-C7010-FAB1-BUN	N7K-C7010-FAB1-BUN	Cisco	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module	3
N7K-SUP1-BUN	N7K-SUP1-BUN	Cisco	Nexus 7000 - Supervisor 1, Includes External 8GB Flash	2
CAB-AC-2500W-US1	CAB-AC-2500W-US1	Cisco	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	6
CON-SNTP-C701BR	CON-SNTP-C701BR	Cisco	SMARTNET 24X7X4 Nexus 7010 Bundle	1
N7K-M132XP-12	N7K-M132XP-12	Cisco	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)	3
N7K-M148GT-11	N7K-M148GT-11	Cisco	Nexus 7000 - 48 Port 10/100/1000, RJ-45	1
N7KS1K9-50	N7KS1K9-50	Cisco	Cisco NX-OS Release 5.0	1

APPENDIX C

Cisco Products and Software Versions

	Device DNS Name	Model	Current Software
Stores			
	FW-A2-MSP-1	ASA5510	asa841-k8.bin
	R-A2-Conv-1	CISCO891W	c890-universalk9-mz.151-3.T.bin
	R-A2-Mini-1	CISCO1941W-A/K9	c1900-universalk9-mz.SPA.151-3.T.bin
	R-A2-Small-1	CISCO2921/K9	c2900-universalk9-mz.SPA.151-3.T.bin
	R-A2-Med-1	CISCO2951 (STARSCREAM Rev 1)	c2951-universalk9-mz.SPA.151-3.T.bin
	R-A2-Med-2	CISCO2951/K9	c2951-universalk9-mz.SPA.151-3.T.bin
	R-A2-Lrg-1	C3945-SPE150/K9	c3900-universalk9-mz.SPA.151-3.T.bin
	R-A2-Lrg-2	C3945-SPE150/K9	c3900-universalk9-mz.SPA.151-3.T.bin
Internet Edge			
	RIE-1	CISCO7206VXR-NPE-G1	c7200-advipservicesk9-mz.124-24.T4.bin
	RIE-2	CISCO7206	c7200p-advipservicesk9-mz.124-11.T3.bin
	RIE-3	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXI5.bin
	RIE-3_FWSM	WS-SVC-FWM-1	c6svc-fwm-k9.4-1-5.bin
	RIE-3_IDSM	WS-SVC-IDSM-2	7.0(4)
	RIE-4	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXI5.bin
	RIE-4_FWSM	WS-SVC-FWM-1	4.1(5)
	RIE-4_IDSM	WS-SVC-IDSM-2	7.0(4)
	ASA-IE-1	ASA5540 w/SSM-40	asa841-k8.bin
	ASA-IE-2	ASA5540 w/SSM-CSC-10	asa841-k8.bin
	IRONPort	Ironport C670	v7.1.3-010
Data Center			

	RWAN-1	ASR-1002 (RP1)	asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin
	RWAN-2	ASR-1002 (RP1)	asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin
	ASA-WAN-1	ASA5540 w/SSM-20	asa841-k8.bin
	ASA-WAN-2	ASA5540 w/SSM-20	asa841-k8.bin
	RCORE-1	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RCORE-2	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RAGG-1	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-1_VDC1	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-1_VDC2	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-2	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-2_VDC1	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-2_VDC2	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	DC-ASA-1_Admin	ASA-5585	asa824-smp-k8.bin
	DC-ASA-1_VDC1	ASA-5585	asa824-smp-k8.bin
	DC-ASA-1_VDC2	ASA-5585	asa824-smp-k8.bin
	DC-ASA-2_Admin	ASA-5585	asa824-smp-k8.bin
	DC-ASA-2_VDC1	ASA-5585	asa824-smp-k8.bin
	DC-ASA-2_VDC2	ASA-5585	asa824-smp-k8.bin
	RSERV-1	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RSERV-1_FWSMa	WS-SVC-FWM-1	4.1(5)
	RSERV-1_FWSMb	WS-SVC-FWM-1	7.0(4) - PwrDown
	RSERV-1_IDSM	WS-SVC-IDSM-2	7.0(4)
	RSERV-1_ACE	ACE20-MOD-K9	A2(1.2)
	RSERV-2	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RSERV-2_FWSMa	WS-SVC-FWM-1	4.1(5)
	RSERV-2_FWSMb	WS-SVC-FWM-1	7.0(4) - PwrDown
	RSERV-2_IDSM	WS-SVC-IDSM-2	7.0(4)

	RSERV-2_ACE	ACE20-MOD-K9	A2(1.2)
Stores			
	S-A2-MSP-1	WS-C3560E-PS-24	c3560e-universalk9-mz.122-35.SE5.bin
	A-A2-MSP-1	AIR-CAP3502I	
	S-A2-Conv-1	WS-C2960PD-8TT-L	c2960-lanbasek9-mz.122-55.SE1.bin
	S-A2-Mini-1	WS-C2960G-8TC-L	c2960-lanbasek9-mz.122-50.SE4.bin
	S-A2-Mini-2	WS-C2960-8TC-L	c2960-lanbasek9-mz.122-50.SE4.bin
	A-A2-Mini-1	AIR-CAP3502E	
	S-A2-Small-1	WS-C2960S-48FPS-L	c2960s-universalk9-mz.122-53.SE1.bin
	S-A2-Small-2 (Stacked)	WS-C2960S-48FPS-L	c2960s-universalk9-mz.122-53.SE1.bin
	A-A2-Small-1	AIR-CAP3502I	
	S-A2-Med-1	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	S-A2-Med-2 (Stacked)	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	S-A2-Med-3	WS-C2960CPD-8PT-L	c2960c405-universalk9-mz.122-55.0.43.SK.bin
	A-A2-Med-1	AIR-CAP3502E	
	A-A2-Med-2	AIR-LAP1262N	
	S-A2-Lrg-1	WS-4507+R SUP-7	cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
	S-A2-Lrg-2	WS-4507+R SUP-7	cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
	S-A2-Lrg-3	WS-C3560X-48PF-S	c3560e-universalk9-mz.122-53.SE2.bin
	S-A2-Lrg-4	WS-C3560X-48PF-S	c3560e-universalk9-mz.122-53.SE2.bin
	S-A2-Lrg-5	WS-C3560CPD-8PT-L	c3560c405ex-universalk9-mz.122-55.0.44.SK.bin
	A-A2-Lrg-1	AIR-CAP3502E	
	A-A2-Lrg-2	AIR-CAP3502I	
	SLC-A2-Lrg-1	AIR-CT5508-12-K9	7.0.114.112
	WAVE-A2-Lrg-1	WAVE-547	
Data Center			
	SWAN-1/2	WS-C3750-48P	c3750-ipbasek9-mz.122-55.SE1.bin
	SWAN-3/4	WS-C3750-48P	c3750-ipbasek9-mz.122-55.SE1.bin
	SACCESS-1	WS-C4948-10GE	cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
	SACCESS-2	WS-C4948-10GE	cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
	SACCESS-3	Nexus5020 Chassis ("40x10GE/Supervisor")	n5000-uk9.5.0.3.N1.1b.bin
	SACCESS-4	Nexus5020 Chassis ("40x10GE/Supervisor")	n5000-uk9.5.0.3.N1.1b.bin
	SACCESS-5	WS-C3750E	c3750e-universalk9-mz.122-40.SE.bin
	F-UCS-1	UCS6120-Fabric	4.1(3)N2(1.3p)
	F-UCS-2	UCS6120-Fabric	4.1(3)N2(1.3p)

	MDS-DC-1	MDS 9506 ("Supervisor/Fabric-2")	m9500-sf2ek9-mzg.5.0.1a.bin.S4
	MDS-DC-2	MDS 9506 ("Supervisor/Fabric-2")	m9500-sf2ek9-mz.5.0.4.bin
	AW-DC-1	AIR-WLC5508-12	7.0.114.112
	AW-DC-2	AIR-WLC5508-12	7.0.114.112
	MSE-DC-1	MSE3550	7.0.200.125
	MSE-DC-2	MSE3550	7.0.200.125
	WAE-DC-1	WAE-7341	
	WAE-DC-2	WAE-7341	
	WAE-DC-3	WAE-602	
	WAE-DC-4	WAE-602	
	Nexus 1kv	Nexus 1kv	4.2(1)SV1(4)
	Nexus VSG	Nexus VSG	4.2(1)VSG1(1)
	Cisco ISE	Cisco Identity Service Engine	1.0.3.377
	WCS Manager	Cisco WCS Manager	7.0.171.107
	CS Manager	Cisco Security Manager	4.0.1
	CS ACS	Cisco Secure Access Control Server	Release 4.2(1) Build 15 Patch 3
	Cisco UCS Manager	Cisco UCS Manager	1.3(1p)
	Cisco UCM	Cisco Unified Communications Manager	8.5.1.11001-3
	EMC NCM	EMC Ionix Network Configuration Manager	4.1.0.863 HF7
	EMC UIM	EMC Unified Infrastructure Manager'	2.0.1.1.160
	EMC Unisphere	EMC Unisphere	1.0.50.1.0326
	RSA DPM	RSA Data Protection Manager	KM-3.1 / AM-6.1.SP3
	RSA enVision	RSA enVision	RSA enVision 4.0 , Revision 5
	RSA Authentication Manager	RSA Authentication Manager	7.1 Service Pack 2
	RSA Archer	RSA Archer	4.5.5
	HyTrust	HyTrust	2.2.1.14064
	VSOM	Cisco Video Surveliance Manager	6.3.1
	PAM	Cisco Physical Access Manager	1.2.0

APPENDIX B

Verizon Business Reference Architecture Report—Cisco PCI Solution for Retail

Based on PCI DSS v. 2.0

06/24/2011

Table of Contents

Contact Information

Verizon Business **Rob McIndoe** *Sr. Security Consultant* *CISSP, PCI QSA, PA-QSA, CISA, GSEC* robert.mcindoe@verizonbusiness.com	
Cisco *Customer contact information*	**Customer logo**

1. Executive Summary

Architecture Description

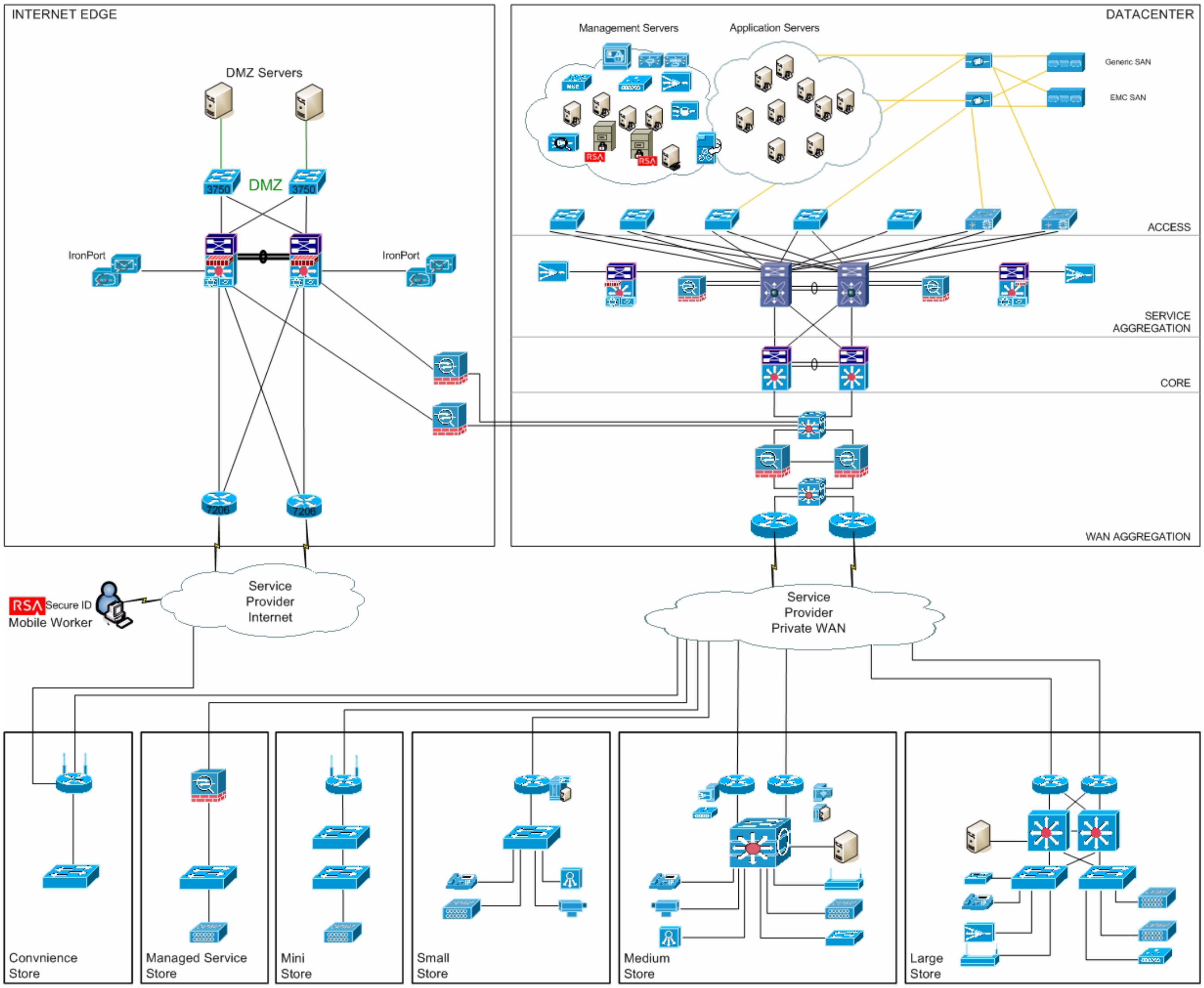
Cisco Systems, Inc engaged Verizon Business to conduct a PCI reference architecture assessment of their "PCI Solution for Retail" designed architecture, based on the PCI DSS v2.0 standard. The architecture assessment against the PCI DSS v2.0 standard included a review of the Cisco PCI Solution for retail network architecture, configurations, security applications, and web management consoles.

Cisco Systems, Inc. will continue to market the assessed reference architecture solution to retail customers looking to meet PCI requirements, specifically within their retail environment and within their back-end data center infrastructure. Cisco has used findings from the assessment to ensure configurations within their solution meet PCI requirements specific to their solution, and plan to provide the results of the assessment to Cisco Sales Engineers interfacing with retail customers.

Verizon Business' assessment covered three PCI retail architectures, targeted to small, medium, and large retail environments. Verizon Business found the three solution architectures to address several technical PCI requirements, and can address other requirements either as a compensating control, or in conjunction with compensating controls depending on organizations infrastructure requirements. The retail architectures are designed to be deployed within a POS retail location, with central management/logging components deployed in a data center environment.

As Cisco's PCI Solution for Retail architecture only addresses some aspects of a merchant's overall PCI compliance responsibility, several areas of PCI compliance are left to the merchant to obtain full compliance. The overall approach to the assessment was to focus validation efforts on components which are core to Cisco's PCI Solution for Retail environment. System components outside of the Cisco PCI Solution for Retail environment (e.g. corporate email, corporate Internet/DMZ firewalls, central cardholder databases, POS systems, mainframes, and corporate networks) were not included in the scope of the assessment.

High Level Network Diagram



Quarterly Vulnerability Scans

N/A - Quarterly scanning (internal and external) is the responsibility of the merchant/service provider, and was not part of the assessment.

2. Description of Scope of Work and Approach Taken

PCI DSS Version

PCI DSS v.2.0 was used for the reference architecture review.

Timeframe

The review took place through several remote interviews and remote validation:

- 3 /1/2011–4/10/2011

Environment on which Assessment Focused

The architecture assessment included the following components:

- **Cisco Routers** (ISR)—891w-AGN, 1941w, ISR G2, 2921/51 ISR G2, 3945 ISR G2, ASR1000, and 7206VXR ISRs are configured with Firewall and IDS feature set.
- **Cisco Switches**—2960 PD-8TT-L, 2960- 8TC-L, 2960 S, 2960 C, 3560 C, 3560 X, 3750 X, 4507-Sup 7, 4948, 6500, Nexus1000v, Nexus5000, Nexus7000, MDS 9500
- **MDS Switch Fabric**
- **Cisco Wireless** —1262N Access Points, 3502E Access Points, 3502I Access Points, CT5508 Controller, WLC2125 Controller, Mobility Service Engine, WCS-Wireless Manager
- **Cisco Security devices**—ASA 5510, ASA 5540, ASA 5580, NAC, IOS Firewall, AnyConnect - VPN.
- **Server Vitalization**—Servers - ISR SRE 900, UCS Express ESXi
- **VBlock**—UCS - MDS - EMC SAN
- **Cisco Security Manager**—Central provisioning of device configuration and security policies, including: ASAs, Cisco Firewall Services Modules, IDS, ISRs, and switches
- **Cisco Secure Access Control Server** (ACS)—AAA server
- **LAN Management Solution** (LMS)—Infrastructure Management
- **RSA Access Manager**—Used for central authentication/logging for access to RSA Data Protection Manager within the assessed environment.
- **RSA Authentication Manager**—Central management/logging of RSA SecurID (two-factor) authentication for remote access into the data center environment.
- **RSA Data Protection Manager (**formerly RSA Key Manager**)**

- **RSA enVision**—RSA's solution for compliance and security information management. RSA enVision was used to centrally collect RSA SecurID authentication logs on the RSA Authentication Manager server, using a batch process that runs several times a day.
- **HyTrust**—Network-based virtual infrastructure policy enforcement. Administrative access control, enforcement of policy across virtual infrastructure, hypervisor hardening, and audit logging. Access and User administration, change and configuration, and operations
- **EMC Ionix NCM**—Built-in compliance template(s) for PCI (and other regulatory requirements). Detects "at-risk" devices according to published vulnerabilities

Network Segmentation

Cisco has designed three network architectures for small, medium, and large retail environments. Cisco has chosen Cisco Integrated Services Routers (ISRs) to provide firewall, IDS/, and routing functionality. Access-lists are applied through firewall policies, which are pushed to the ISRs in each architecture. Access-lists implicitly deny all inbound and outbound traffic to the PCI Solution for Retail; all traffic approved within each design is explicitly allowed to the IP address, port and service level. Additionally, Cisco has incorporated wireless into the design, using WPA-TKIP for secure wireless networking.

The data center environment is segmented into multiple VLANs, including Internet Edge, WAN aggregation, and Core service aggregation. Multiple layers of network security are included in all data center segments, including Cisco Firewall Services Module and ASA stateful firewall filtering and integrated IDS/ detection/prevention, access lists, secure VPN (WAN aggregation and remote VPN), and two-factor authentication.

All network devices within the PCI Solution for Retail are centrally managed through the following:

- Cisco Security Manager (CSM) - (Central security management for ISRs and switches (e.g., firewall policy, IDS/signatures))
- Cisco Wireless Control System (WCS)—(Central wireless management)
- Cisco ACS—Central TACACS+ (central authentication) server for ASA firewall, Cisco Firewall Services Module, ISR, 7206 VXR router, switch, wireless controller (RSA enVision and WCS).
- RSA enVision—Central logging/Correlation/Analysis/Alerting server. Alerts from IDS/alerts and firewall logs.
- Cisco ASDM—Central configuration for ASA firewalls.
- Cisco Device Manager (IDM)—IDS/configuration management.

Exclusions

Due to the nature of this assessment, several areas of a normal PCI assessment were excluded, including:

- Central cardholder data storage
- Authorization/settlement processes
- Policies, procedures, and standards
- Assessment of "in transit" cardholder data
- Physical security
- SDLC policies and procedures

- Live cardholder transactions (a POS environment, which includes authorization responses, was not available during the assessment)

Wireless LANs and/or Wireless Applications

Wireless networks within the PCI Solution for Retail environment have been configured to use WPA-TKIP authentication for secure wireless networking. All wireless traffic must pass through the ISRs and IOS firewall access-lists to traverse any part of the PCI Solution for Retail network. Additionally, best practice security parameters have been applied to wireless networks, including: HTTPS access for wireless management, default SSID has been changed, SNMPv3 used (default strings changed), and HTTP access has been disabled.

List of Individuals Interviewed

The following staff was interviewed:

Interviewee(s)	Title
Christian Janoff, Bart Mcglothin	Network architecture, firewalls, routers, switches, wireless, IDS/
Christian Janoff, Bart Mcglothin	Audit Logging
Christian Janoff, Bart Mcglothin	Access Control / Authentication
Christian Janoff, Bart Mcglothin	CSM
Tom Hua	CSM
Christian Janoff, Bart Mcglothin	Wireless
Christian Janoff, Bart Mcglothin	LMS
Rupesh Chakkingal,	RSA Data Protection Manager
Rupesh Chakkingal	RSA Data Protection Manager
Bart Mcglothin	Cisco ASA – Secure configuration reviews
Sheri Spence	EMC SAN
Syed Ghayur	Nexus 1kv
Mike Adler	Wireless lab
Sujit Ghosh	Wireless lab
K. Sigel	HyTrust
R. Budko	HyTrust
Christian Janoff, Bart Mcglothin	Cisco Virtual Service Gateway
Syed Ghayur	Cisco Virtual Service Gateway
David Valiquette	RSA
Manual Kamer	EMC Ionix
Pandit Panburana	CUCM
Mourad Cherfaoui	CUCM

Danny Dhillon	RSA enVision
Danny Dhillon	RSA Authentication Manager
Danny Dhillon	RSA Data Protection Manager, RSA Access Manager, RSA Authentication Manager

List of Documents Reviewed

The following documents were reviewed:

Document	Date
Enterprise Retail PCI DSS 2.0.pdf	11/17/2010
switch and router configs	04/15/11
Switch configs - stores	04/15/11
Common requirements questions across all devices.xls	12/01/10
Products Alignment_2010-10-13.xlsx	10/13/10
PCI Retail Solution Products.xlsx	04/15/11

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity’s networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity’s internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity’s trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
1.1 Establish firewall and router configuration standards that include the following:	**1.1** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider.		
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.	Verizon Business reviewed network diagrams and verified that they document all connections to cardholder data, including any wireless networks.		**Note:** Since each network environment will be unique to the merchant or service provider, updating network diagrams remains the responsibility of each merchant / service provider
	1.1.2.b Verify that the diagram is kept current.	Verizon Business reviewed network diagrams and verified that they kept current.		**Note:** Since each network environment will be unique to the merchant or service provider, updating network diagrams remains the responsibility of each merchant / service provider
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3.a** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider.		
	1.1.3.b Verify that the current network diagram is consistent with the firewall configuration standards.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider.		

1.1.4 Description of groups, roles, and responsibilities for logical management of network components	**1.1.4** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider. **Note:** Verizon Business confirmed role-based groups were created within Cisco ACS for logical management of network devices (e.g. Administrator, System Monitoring, and Config Manager groups).		
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.	**1.1.5.a** Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider. **Note:** Verizon Business reviewed access-lists, in addition to a documented list of required services/protocols for the PCI Solution for Retail environment, and confirmed traffic is limited to that which is required for the environment.		
	1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider.		
1.1.6 Requirement to review firewall and router rule sets at least every six months	**1.1.6.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider.		
	1.1.6.b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.	N/A – Firewall/Router configuration standards (documentation) is the responsibility of the merchant / service provider.		

1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. **Note:** An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.	**1.2** Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:			

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	**1.2.1.a** Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.	Verizon Business reviewed access lists across firewalls and routers and verified that inbound and outbound traffic is limited to that which is necessary for a cardholder data environment. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945		Configurations for perimeter firewalls/routers outside the PCI Solution for Retail environment are the responsibility of merchant / service provider.
	1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.	Verizon Business reviewed access lists across firewalls and routers and verified that all other inbound and outbound traffic is specifically denied. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945		

1.2.2 Secure and synchronize router configuration files.	**1.2.2** Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.	Verizon Business reviewed router configuration and verified that configuration files are secure and synchronized. Verizon Business observed system-generated configuration output for the following system components: Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206		
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	**1.2.3** Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	Verizon Business confirmed that the PCI Reference Architecture for Retail Solutions was designed and segmented to require all wireless traffic destined for any wired host (WCS Manager), to pass through firewall access-lists before being permitted. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945		

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	**1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—to determine that there is no direct access between the Internet and system components in the internal cardholder network segment, as detailed below.			
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**1.3.1** Verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	Verizon Business reviewed network topologies and access lists across firewalls and routers and verified that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Services Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540		

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	**1.3.2** Verify that inbound Internet traffic is limited to IP addresses within the DMZ.	Verizon Business reviewed static IPs, and access lists across firewalls and routers and verified that that inbound Internet traffic is limited to IP addresses within the DMZ. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206		Perimeter firewall/router configurations and rule sets are the responsibility of the merchant / service provider.

1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	**1.3.3** Verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.	Verizon Business reviewed network diagrams, configurations from network-infrastructure system components, including wireless APs and verified that direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206		

1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.	**1.3.4** Verify that internal addresses cannot pass from the Internet into the DMZ**.**	Verizon Business reviewed access-lists on the Internet edge router and confirmed that Internet sourced RFC-1918 addresses are explicitly denied and that internal addresses cannot pass from the Internet into the DMZ. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206		

1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**1.3.5** Verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized	Verizon Business reviewed outbound access-lists from the PCI Reference Architecture for Retail Solutions environment and confirmed that all outbound traffic is destined for "data center" systems. There is no outbound Internet access from the PCI Reference Architecture for Retail Solutions environment. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206		

1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)	**1.3.6** Verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.)	Verizon Business confirmed the PCI Solution for Retail environment configurations for the Cisco ASA firewalls, Cisco Virtual Service Gateways, Cisco Firewall Services Modules, and ISRs with a firewall feature set were configured to perform stateful packet inspections. Verizon Business observed system-generated configuration output for the following system components: Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206		

1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**1.3.7** Verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.	Verizon Business reviewed network topologies, network diagrams, and access lists across firewalls and routers and verified that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206		

1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* *Network Address Translation (NAT)* *Placing servers containing cardholder data behind proxy servers/firewalls or content caches,* *Removal or filtering of route advertisements for private networks that employ registered addressing,* *Internal use of RFC1918 address space instead of registered addresses.*	**1.3.8.a** Verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	Verizon Business reviewed DHCP reservations, static IPs, and access lists across firewalls and routers and confirmed that RFC 1918 addresses were used within the PCI Solution for Retail environment. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206		
	1.3.8.b Verify that any disclosure of private IP addresses and routing information to external entities is authorized.	N/A – Policies and procedures is the responsibility of the merchant / service provider.		

1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	**1.4.a** Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active.	**N/A** – Security Policy (Remote Access – Desktop firewalls) is the responsibility of the merchant / service provider. Installation of personal firewall software for any mobile and employee-owned computers with direct Internet connectivity, and which are used to access the merchant / service provider network, is the responsibility of the merchant / service provider.		
	1.4.b Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by users of mobile and/or employee-owned computers.	**N/A** – Security Policy (Remote Access – Desktop firewalls) is the responsibility of the merchant / service provider. Installation of personal firewall software for any mobile and employee-owned computers with direct Internet connectivity, and which are used to access the merchant / service provider network, is the responsibility of the merchant / service provider.		

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
2.1 Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	**2.1** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords	Verizon Business observed administrators during the login process, while attempting to logon with default accounts and passwords. Verizon Business confirmed all default passwords, including passwords for interactive administrator accounts and SNMP community strings have been changed. Verizon Business confirmed all default administrator accounts have been removed, where possible. Some default administrator accounts cannot be removed from the system, due to application dependencies; however, unique administrator accounts have been created, in order to eliminate the need to use all default administrator accounts.		
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	**2.1.1** Verify the following regarding vendor default settings for wireless environments:			
	2.1.1.a Verify encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment and verified the following: Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N		
	2.1.1.b Verify default SNMP community strings on wireless devices were changed.	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment and verified the following: Default SNMP community strings have been changed and (SNMPv3 is being used).		

	2.1.1.c Verify default passwords/passphrases on access points were changed.	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment and verified the following: No default passwords exist within the wireless environment. These are entered at initial login. Only unique, non-default accounts exist for interactive administration within the wireless		
	2.1.1.d Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment and verified the following: WPA technology is enabled (WPA/TKIP w/PEAP authentication).		
	2.1.1.e Verify other security-related wireless vendor defaults were changed, if applicable.	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment and verified the following: No Default SSID exists. This must be entered at initial installation, and is recommended by Cisco to be unique. SSID broadcast was disabled. Wireless management and web mode is disabled.		

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: Center for Internet Security (CIS) International Organization for Standardization (ISO) SysAdmin Audit Network Security (SANS) Institute National Institute of Standards Technology (NIST)	**2.2.a** Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-store Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560E Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager RSA Authentication Manager RSA EnVision Cisco Identity Services Engine EMC CLARiiON CX-240 Cisco Unified Computing System Cisco UCS Express on Services Ready Engine Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control **Note:** Verizon Business reviewed configurations across all above mentioned technologies and confirmed they were configured according to best practice standards.		

	2.2.b Verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.2.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-store Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560E Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager RSA Authentication Manager RSA EnVision Cisco Identity Services Engine EMC CLARiiON CX-240 Cisco Unified Computing System Cisco UCS Express on Services Ready Engine Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control **Note:** Verizon Business reviewed configurations across all above mentioned technologies and confirmed they were configured according to best practice standards.		

	2.2.c Verify that system configuration standards are applied when new systems are configured.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series (Data Center) Cisco ASA 5500 Series (Store) Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-store Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560E Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager RSA Authentication Manager RSA EnVision Cisco Identity Services Engine EMC CLARiiON CX-240 Cisco Unified Computing System Cisco UCS Express on Services Ready Engine Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control **Note:** Verizon Business reviewed configurations across all above mentioned technologies and confirmed they were configured according to best practice standards.		

	2.2.d Verify that system configuration standards include each item below (2.2.1 – 2.2.4).			
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) **Note:** Where virtualization technologies are in use, implement only one primary function per virtual system component.	**2.2.1.a** For a sample of system components, verify that only one primary function is implemented per server.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider. **Note:** Verizon Business reviewed configurations across all above mentioned technologies and confirmed they were configured according to best practice standards.		
	2.2.1.b If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider.		

2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or ec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	**2.2.2.a** For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that only necessary services or protocols are enabled.	Verizon Business reviewed configuration settings for PCI Reference Architecture for Retail Solutions and verified that that only necessary services or protocols are enabled. **Note:** Although Cisco followed a configuration standard to harden the OS for management consoles, Verizon Business did not review those configurations beyond secure administrative access (e.g. https, SSH), audit logging, and password/lockout settings. OS hardening is the responsibility of the merchant / service provider, and would vary significantly, depending on OS platform and POS applications deployed. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Integrated Services Routers (ISRs) Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		.

	2.2.2.b Identify any enabled insecure services, daemons, or protocols. Verify they are justified and that security features are documented and implemented.	Verizon Business reviewed configuration settings for PCI Reference Architecture for Retail Solutions and verified that insecure services and protocols are not used. **Note:** Although Cisco followed a configuration standard to harden the OS for management consoles, Verizon Business did not review those configurations beyond secure administrative access (e.g. https, SSH), audit logging, and password/lockout settings. OS hardening is the responsibility of the merchant / service provider, and would vary significantly, depending on OS platform and POS applications deployed. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Integrated Services Routers (ISRs) Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

2.2.3 Configure system security parameters to prevent misuse.	**2.2.3.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.	Verizon Business interviewed administrators, architects, and SMEs from business units to verify they have knowledge of common security parameters of the system components within the PCI Reference Architecture for Retail Solutions environment.		

	2.2.3.b Verify that common security parameter settings are included in the system configuration standards.	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards) is the responsibility of the merchant / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Video Surveillance Cisco Physical Access Control		Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.

	2.2.3.c For a sample of system components, verify that common security parameters are set appropriately.	Verizon Business reviewed configuration settings across all PCI Reference Architecture for Retail Solutions and confirmed they were based on best practice standards, and that common security parameters were set appropriately. Verizon Business also confirmed all management consoles were configured to support secure access (e.g. SSH, https, High-Encryption RDP), and that http, Telnet, and other insecure protocols commonly used for administrative access had been disabled. Additionally, role-based administration was configured for administration of the PCI Reference Architecture for Retail Solutions. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Video Surveillance Cisco Physical Access Control		Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.

2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2.2.4.a** For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.	Verizon Business reviewed configurations across all PCI Reference Architecture for Retail Solutions and verified that they were based on best practice standards, and that all unnecessary functionality was disabled. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.

	2.2.4.b. Verify enabled functions are documented and support secure configuration.	Verizon Business reviewed configurations across all PCI Reference Architecture for Retail Solutions and confirmed that enabled functions are documented and support secure configuration. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.

	2.2.4.c. Verify that only documented functionality is present on the sampled system components.	Verizon Business reviewed configurations across all PCI Reference Architecture for Retail Solutions and confirmed that only documented functionality is present on the sampled system components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.

2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non- console administrative access.	**2.3** For a sample of system components, verify that non-console administrative access is encrypted by performing the following:			

	2.3.a Observe an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested.	Verizon Business reviewed non-console administrative access for all PCI Reference Architecture for Retail Solutions and verified that strong encryption methods are invoked before the administrator's password is requested. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		**Note:** Verification of telnet presence within the management consoles (Windows Server 2003) was not performed. This is the responsibility of the merchant / service provider, as part of secure configuration standard processes.

	2.3.b Review services and parameter files on systems to determine that Telnet and other remote login commands are not available for use internally.	Verizon Business reviewed non-console administrative access for all PCI Reference Architecture for Retail Solutions and verified that Telnet and other remote login commands are not available for use internally. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		**Note:** Verification of telnet presence within the management consoles (Windows Server 2003) was not performed. This is the responsibility of the merchant / service provider, as part of secure configuration standard processes.

	2.3.c Verify that administrator access to the web-based management interfaces is encrypted with strong cryptography.	Verizon Business reviewed non-console administrative access for all PCI Reference Architecture for Retail Solutions and verified that administrator access to the web-based management interfaces is encrypted with strong cryptography. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco Video Surveillance		**Note:** Verification of telnet presence within the management consoles (Windows Server 2003) was not performed. This is the responsibility of the merchant / service provider, as part of secure configuration standard processes.
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	**2.4** Perform testing procedures **A.1.1** through **A.1.4** detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.	N/A – For the purpose of this assessment, Cisco is not a hosting provider.		

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of “strong cryptography” and other PCI DSS terms.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows.	**3.1** Obtain and examine the policies, procedures and processes for data retention and disposal, and perform the following:			

3.1.1 Implement a data retention and disposal policy that includes: Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements Processes for secure deletion of data when no longer needed Specific retention requirements for cardholder data A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements	**3.1.1.a** Verify that policies and procedures are implemented and include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons).	N/A – Data retention / Data disposal policy and procedures is the responsibility of the merchant / service provider.		
	3.1.1.b Verify that policies and procedures include provisions for secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data.	N/A – Data retention / Data disposal policy and procedures is the responsibility of the merchant / service provider.		
	3.1.1.c Verify that policies and procedures include coverage for all storage of cardholder data.	N/A – Data retention / Data disposal policy and procedures is the responsibility of the merchant / service provider.		
	3.1.1.d Verify that policies and procedures include at least one of the following: A programmatic process (automatic or manual) to remove, at least quarterly, stored cardholder data that exceeds requirements defined in the data retention policy. Requirements for a review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements defined in the data retention policy.	N/A – Data retention / Data disposal policy and procedures is the responsibility of the merchant / service provider.		

	3.1.1.e For a sample of system components that store cardholder data, verify that the data stored does not exceed the requirements defined in the data retention policy.	N/A – Data retention / Data disposal policy and procedures is the responsibility of the merchant / service provider.		
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: **Note:** It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.	**3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, verify there is a business justification for the storage of sensitive authentication data, and that the data is secured.	N/A – Cisco is not an Issuer and does not support issuing services.		
	3.2.b For all other entities, if sensitive authentication data is received and deleted, obtain and review the processes for securely deleting the data to verify that the data is unrecoverable.	N/A – It is the responsibility of the merchant to ensure systems used do not store sensitive authentication data (e.g. full track data, CVV2, PIN/PIN block) post authorization (even if encrypted).		
	3.2.c For each item of sensitive authentication data below, perform the following steps:			

3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. **Note:** In the normal course of business, the following data elements from the magnetic stripe may need to be retained: The cardholder's name Primary account number (PAN) Expiration date Service code To minimize risk, store only these data elements as needed for business.	**3.2.1** For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored under any circumstance: Incoming transaction data All logs (for example, transaction, history, debugging, error) History files Trace files Several database schemas Database contents	N/A – It is the responsibility of the merchant to ensure systems used do not store sensitive authentication data (e.g. full track data, CVV2, PIN/PIN block) post authorization (even if encrypted).		
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not- present transactions.	**3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three- digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance: Incoming transaction data All logs (for example, transaction, history, debugging, error) History files Trace files Several database schemas Database contents	N/A – It is the responsibility of the merchant to ensure systems used do not store sensitive authentication data (e.g. full track data, CVV2, PIN/PIN block) post authorization (even if encrypted).		
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	**3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance: Incoming transaction data All logs (for example, transaction, history, debugging, error) History files Trace files Several database schemas Database contents	N/A – It is the responsibility of the merchant to ensure systems used do not store sensitive authentication data (e.g. full track data, CVV2, PIN/PIN block) post authorization (even if encrypted).		

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). **Notes:** This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.	**3.3** Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.	N/A – Data control and Data classification policies and procedures, including masking PAN data, except for those with a specific need to see full PAN data, is the responsibility of the merchant.		

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: One-way hashes based on strong cryptography (hash must be of the entire PAN) Truncation (hashing cannot be used to replace the truncated segment of PAN) Index tokens and pads (pads must be securely stored) Strong cryptography with associated key-management processes and procedures **Note:** It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	**3.4.a** Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using any of the following methods: One-way hashes based on strong cryptography Truncation Index tokens and pads, with the pads being securely stored Strong cryptography, with associated key-management processes and procedures	N/A – Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the merchant / service provider. Verizon Business reviewed RSA Data Protection Manager application, related to protecting sensitive data within Cisco's PCI Solution for Retail environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable RSA Data Protection Manager – 192-bit 3DES or 256-bit AES encryption. RSA Data Protection Manager – 192-bit 3DES or 128-bit, 192-bit, or 256-bit AES encryption.		
	3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).	N/A – Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the merchant / service provider.		
	3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.	N/A – Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the merchant / service provider.		
	3.4.d Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs.	N/A – Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the merchant / service provider.		

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	**3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).	Verizon Business reviewed RSA Data Protection Manager, EMC CLARiiON CX-240, Cisco MDS Storage Switches, related to protecting sensitive data within Cisco's PCI Solution for Retail environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable. **Note**: Although the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these switches provide the capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.		
	3.4.1.b Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).	Verizon Business reviewed RSA Data Protection Manager, EMC CLARiiON CX-240, Cisco MDS Storage Switches, related to protecting sensitive data within Cisco's PCI Solution for Retail environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable. **Note**: Although the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these switches provide the capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.		

	3.4.1.c Verify that cardholder data on removable media is encrypted wherever stored. **Note:** If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.	Verizon Business reviewed RSA Data Protection Manager, EMC CLARiiON CX-240, Cisco MDS Storage Switches, related to protecting sensitive data within Cisco's PCI Solution for Retail environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable. **Note**: Although the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these switches provide the capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.		
3.5 Protect any keys used to secure cardholder data against disclosure and misuse: **Note:** This requirement also applies to key-encrypting keys used to protect data- encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.	**3.5** Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:			

3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	**3.5.1** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.	N/A – Protection of encryption keys is the responsibility of the merchant / service provider. Verizon Business confirmed that restricted access to encryption keys is as follows RSA Data Protection Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported to a key administrator. RSA Data Protection Manager security policies require public key authentication to access key material for encryption/decryption purposes. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	**3.5.2.a** Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.	N/A – Protection of encryption keys is the responsibility of the merchant / service provider. RSA Data Protection Manager: Key encryption key is stored in memory and data encryption keys are stored in encrypted format within Oracle or MS SQL database. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		
	3.5.2.b Identify key storage locations to verify that keys are stored in the fewest possible locations and forms.	N/A – Protection of encryption keys is the responsibility of the merchant / service provider. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: **Note:** Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.	**3.6.a** Verify the existence of key-management procedures for keys used for encryption of cardholder data.	N/A – Key Management policy and procedures is the responsibility of the merchant / service provider.		
	3.6.b For service providers only: If the service provider shares keys with their customers for transmission or storage of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely transmit, store and update customer's keys, in accordance with Requirements 3.6.1 through 3.6.8 below.	N/A – Key Management policy and procedures is the responsibility of the merchant / service provider.		
	3.6.c Examine the key-management procedures and perform the following:			
3.6.1 Generation of strong cryptographic keys	**3.6.1** Verify that key-management procedures are implemented to require the generation of strong keys.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that generation of strong keys is included for the following: RSA Data Protection Manager: 192-bit 3DES or 128-bit/192-bit/256-bit AES keys Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6.2 Secure cryptographic key distribution	**3.6.2** Verify that key-management procedures are implemented to require secure key distribution.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that secure distribution of keys is included for the following: RSA Data Protection Manager: All key transfers are done over SSLv3/TLSv1 connections between Key Manager Server and Key Manager Clients. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6.3 Secure cryptographic key storage	**3.6.3** Verify that key-management procedures are implemented to require secure key storage.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that secure key storage is included for the following: RSA Data Protection Manager: Key encryption key is stored in memory and data encryption keys are stored in encrypted format within Oracle or MS SQL database. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher- text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	**3.6.4** Verify that key-management procedures are implemented to require periodic key changes at the end of the defined cryptoperiod.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that key rotation capabilities are included for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined. Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. **Note:** If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.	**3.6.5.a** Verify that key-management procedures are implemented to require the retirement of keys when the integrity of the key has been weakened.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that destruction of keys is included for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined, or delete, when necessary.		
	3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that replacement of known or suspected compromised keys is included for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined necessary.		

	3.6.5.c If retired or replaced cryptographic keys are retained, verify that these keys are not used for encryption operations.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that retired or replaced cryptographic keys are retained, and that these keys are not used for encryption operations for the following: RSA Data Protection Manager: RSA Data Protection Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined Verizon Business observed system-generated configuration output for the following system components: RSA Data Protection Manager Cisco MDS Storage Switches		

3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). **Note:** Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	**3.6.6** Verify that manual clear-text key-management procedures require split knowledge and dual control of keys.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that split knowledge/dual control of keys is included for the following: RSA Data Protection Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format.		

3.6.7 Prevention of unauthorized substitution of cryptographic keys.	**3.6.7** Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.	N/A – Key Management policies and procedures is the responsibility of the merchant / service provider. Verizon Business confirmed that prevention of unauthorized substitution of keys is included for the following: RSA Data Protection Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format. Key administration functions can only be access through the Key Manager server, via access controls (authentication) through the RSA Access Manager server.		
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	**3.6.8** Verify that key-management procedures are implemented to require key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	N/A – Key custodian lists are the responsibility of the merchant/service provider.		

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments

4.1 Use strong cryptography and security protocols (for example, SSL/TLS, EC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to: The Internet Wireless technologies, Global System for Mobile communications (GSM) General Packet Radio Service (GPRS)	**4.1** Verify the use of security protocols wherever cardholder data is transmitted or received over open, public networks. Verify that strong cryptography is used during data transmission, as follows:	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions and verified that it uses security protocols wherever cardholder data is transmitted or received over open, public networks. **Note:** Wireless networks have been configured to provide PCI required security necessary to support cardholder traffic. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N		
	4.1.a Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit.	**Note:** Verizon Business reviewed wireless settings within the PCI Solution for Retail environment to confirm WPA encryption has been implemented for all wireless traffic.		
	4.1.b Verify that only trusted keys and/or certificates are accepted.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions and verified that that only trusted keys and/or certificates are accepted.		

	4.1.c Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions and verified that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.		
	4.1.d Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions and verified that the proper encryption strength is implemented for the encryption methodology in use.		
	4.1.e For SSL/TLS implementations: Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). Verify that no cardholder data is required when HTTPS does not appear in the URL.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions and verified that for SSL/TLS implementations, HTTPS appears as a part of the browser URL		
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. **Note:** The use of WEP as a security control was prohibited as of 30 June 2010.	**4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.	Verizon Business reviewed wireless settings within the PCI Reference Architecture for Retail Solutions environment to confirm that WPA encryption has been implemented for all wireless traffic. Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N		

4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	**4.2.a** Verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	N/A – Data Control / Encryption policy and procedures is the responsibility of the merchant / service provider.		
	4.2.b Verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.	N/A – Data Control / Encryption policy and procedures is the responsibility of the merchant / service provider.		

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business- approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	N/A – Deployment of anti-virus software on all servers within the PCI Reference Architecture for Retail Solutions environment is the responsibility of the merchant / service provider.		
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**5.1.1** For a sample of system components, verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).	N/A – Deployment of anti-virus software on all servers within the PCI Reference Architecture for Retail Solutions environment is the responsibility of the merchant / service provider.		

5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	**5.2** Verify that all anti-virus software is current, actively running, and generating logs by performing the following:	N/A – Deployment of anti-virus software on all servers within the PCI Reference Architecture for Retail Solutions environment is the responsibility of the merchant / service provider.		
	5.2.a Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.	N/A – Written A/V policy is the responsibility of the merchant / service provider.		
	5.2.b Verify that the master installation of the software is enabled for automatic updates and periodic scans.	N/A – Deployment of anti-virus software on all servers within the PCI Reference Architecture for Retail Solutions environment is the responsibility of the merchant / service provider.		
	5.2.c For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled.	N/A – Deployment of anti-virus software on all servers within the PCI Reference Architecture for Retail Solutions environment is the responsibility of the merchant / service provider.		
	5.2.d For a sample of system components, verify that antivirus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7	N/A – Central storage and retention of A/V logs is the responsibility of the merchant / service provider.		

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor- provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: *Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.*

PCI DSS Requirements	Testing Procedures	In Place	Not In Place	Comments

6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. **Note:** An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.	**6.1.a** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.	Verizon Business reviewed configurations for the PCI Reference Architecture for Retail Solution components, including management consoles for components within the PCI Solution for Retail environment and confirmed they are running current software releases and contain current vendor patches as of the time of this assessment. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.	N/A – Patch management policy and procedures is the responsibility of the merchant / service provider.		
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. **Notes:** Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component. The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.	**6.2.a** Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities, and that a risk ranking is assigned to such vulnerabilities. (At	N/A – Patch / Risk management policy and procedures is the responsibility of the merchant / service provider.		
	6.2.b Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information.	N/A – Patch / Risk management policy and procedures is the responsibility of the merchant / service provider. Verizon Business recommends using multiple outside sources (e.g. SANS, CERT, SecurityFocus, vendor websites, etc) to identify new vulnerability issues within the environment.		

6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:	**6.3.a** Obtain and examine written software development processes to verify that the processes are based on industry standards and/or	N/A – Software Development was not in scope for this assessment.		
	6.3.b Examine written software development processes to verify that information security is included throughout the life cycle.	N/A – Software Development was not in scope for this assessment.		
	6.3.c Examine written software development processes to verify that software applications are developed in accordance with	N/A – Software Development was not in scope for this assessment.		
	6.3.d From an examination of written software development processes, and interviews of software developers, verify			
6.3.1 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	**6.3.1** Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to	N/A – Software Development was not in scope for this assessment.		

6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. **Note:** This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	**6.3.2.a** Obtain and review policies to confirm that all custom application code changes must be reviewed (using either manual or automated processes) as follows: Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). Appropriate corrections are implemented prior to release.	N/A – Software Development was not in scope for this assessment.		
	6.3.2.b Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above.	N/A – Software Development was not in scope for this assessment.		

6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	**6.4** From an examination of change control processes, interviews with system and network administrators, and examination of relevant data (network configuration documentation, production and test data, etc.), verify the following:			
6.4.1 Separate development/test and production environments	**6.4.1** The development/test environments are separate from the production environment, with access control in place to enforce the separation.	N/A – Software Development was not in scope for this assessment.		
6.4.2 Separation of duties between development/test and production environments	**6.4.2** There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.	N/A – Software Development was not in scope for this assessment.		
6.4.3 Production data (live PANs) are not used for testing or development	**6.4.3** Production data (live PANs) are not used for testing or development.	N/A – Software Development was not in scope for this assessment.		
6.4.4 Removal of test data and accounts before production systems become active	**6.4.4** Test data and accounts are removed before a production system becomes active.	N/A – Software Development was not in scope for this assessment.		

6.4.5 Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	**6.4.5.a** Verify that change-control procedures related to implementing security patches and software modifications are documented and require items 6.4.5.1 – 6.4.5.4	N/A – Software Development was not in scope for this assessment.		
	6.4.5.b For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation. For each change examined, perform the			
6.4.5.1 Documentation of impact.	**6.4.5.1** Verify that documentation of impact is included in the change control documentation for each sampled change.	N/A – Security Policy/Procedures (Change Control) is the responsibility of the merchant / service provider.		
6.4.5.2 Documented change approval by authorized parties.	**6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change.	N/A – Security Policy/Procedures (Change Control) is the responsibility of the merchant / service provider.		

6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	**6.4.5.3.a** For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system.	N/A – Security Policy/Procedures (Change Control) is the responsibility of the merchant / service provider.		
	6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.	N/A – Security Policy/Procedures (Change Control) is the responsibility of the merchant / service provider.		
6.4.5.4 Back-out procedures.	**6.4.5.4** Verify that back-out procedures are prepared for each sampled change.	N/A – Security Policy/Procedures (Change Control) is the responsibility of the merchant / service provider.		
6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: **Note:** The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	**6.5.a**Obtain and review software development processes. Verify that processes require training in secure coding techniques for developers, based on industry best practices and	N/A – Software Development is not in scope for assessment.		
	6.5.b Interview a sample of developers and obtain evidence that they are knowledgeable in	N/A – Software Development is not in scope for assessment.		
	6.5.c. Verify that processes are in place to ensure that applications are not vulnerable to, at a minimum, the following:			

6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**6.5.1** Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)	N/A – Software Development is not in scope for assessment.		
6.5.2 Buffer overflow	**6.5.2** Buffer overflow (Validate buffer boundaries and truncate input strings.)	N/A – Software Development is not in scope for assessment.		
6.5.3 Insecure cryptographic storage	**6.5.3** Insecure cryptographic storage (Prevent cryptographic flaws)	N/A – Software Development is not in scope for assessment.		
6.5.4 Insecure communications	**6.5.4** Insecure communications (Properly encrypt all authenticated and sensitive communications)	N/A – Software Development is not in scope for assessment.		
6.5.5 Improper error handling	**6.5.5** Improper error handling (Do not leak information via error messages)	N/A – Software Development is not in scope for assessment.		
6.5.6 All “High” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2).	**6.5.6** All “High” vulnerabilities as identified in PCI DSS Requirement 6.2.	N/A – Software Development is not in scope for assessment.		
Note: Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external):				
6.5.7 Cross-site scripting (XSS)	**6.5.7** Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)	N/A – Software Development is not in scope for assessment.		

6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)	**6.5.8** Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object	N/A – Software Development is not in scope for assessment.		
6.5.9 Cross-site request forgery (CSRF)	**6.5.9** Cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically	N/A – Software Development is not in scope for assessment.		

6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Installing a web-application firewall in front of public-facing web applications	**6.6** For public-facing web applications, ensure that either one of the following methods are in place as follows: Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows: - At least annually - After any changes - By an organization that specializes in application security - That all vulnerabilities are corrected - That the application is re-evaluated after the corrections Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. **Note:** "An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.	N/A – Public-facing web applications are not in scope for assessment.		

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	**7.1** Obtain and examine written policy for data control, and verify that the policy incorporates the following:			

7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	**7.1.1** Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.	Verizon Business confirmed privileged user IDs are restricted to the least privileges necessary to perform job functions and exist for the following components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

7.1.2 Assignment of privileges is based on individual personnel's job classification and function	**7.1.2** Confirm that privileges are assigned to individuals based on job classification and function (also called "role-based access control" or RBAC).	Verizon Business confirmed privileges are assigned to roles that exist for the following components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.	**7.1.3** Confirm that documented approval by authorized parties is required (in writing or electronically) for all access, and that it must specify required privileges.	Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

7.1.4 Implementation of an automated access control system	**7.1.4** Confirm that access controls are implemented via an automated access control system.	Verizon Business confirmed automated access controls exist for the following components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision SSL VPN Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	**7.2** Examine system settings and vendor documentation to verify that an access control system is implemented as follows:			

7.2.1 Coverage of all system components	**7.2.1** Confirm that access control systems are in place on all system components.	Verizon Business reviewed system components and verified that access control systems are in place on all PCI Reference Architecture for Retail Solutions components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

7.2.2 Assignment of privileges to individuals based on job classification and function	**7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.	Verizon Business reviewed system components and verified that access control systems include role-based privilege assignment for all PCI Reference Architecture for Retail Solutions components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

7.2.3 Default "deny-all" setting **Note:** Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.	**7.2.3** Confirm that the access control systems have a default "deny-all" setting.	Verizon Business reviewed system components and verified that access control systems include default "deny-all" settings on all PCI Reference Architecture for Retail Solutions components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 502 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

Requirement 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

Note: *These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. However, Requirements 8.1, 8.2 and 8.5.8 through 8.5.15 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).*

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments

8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**8.1** Verify that all users are assigned a unique ID for access to system components or cardholder data.	Verizon Business reviewed access lists on all PCI Reference Architecture for Retail Solution components and verified that all users are assigned a unique ID for access to system components or cardholder data. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA EnVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: Something you know, such as a password or passphrase Something you have, such as a token device or smart card Something you are, such as a biometric	**8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following: Obtain and examine documentation describing the authentication method(s) used. For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).	Verizon Business reviewed authentication methods, including observation of live login attempts and verified that a unique ID and password was required for each authentication attempt to all PCI Reference Architecture for Retail Solution components. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) **Note:** Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.	**8.3** To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that two of the three authentication methods are used.	Verizon Business reviewed these components and verified that two-factor authentication was used for remote access. Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 RSA Authentication Manager with SecurID **Note**: All products that can use RADIUS authentication would be able to use the two-factor authentication capabilities of RSA Authentication Manager with SecurID.		Two-factor authentication for all remote access, including for employees, contractors, and third parties, is the responsibility of the merchant / service provider.

8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	**8.4.a** For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage.	Verizon Business reviewed configuration settings of all PCI Reference Architecture for Retail Solution components and verified that passwords are unreadable during transmission and storage. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	8.4.b For service providers only, observe password files to verify that customer passwords are encrypted.	N/A – For the purpose of this assessment, Cisco is not a service provider.		
8.5 Ensure proper user identification and authentication management for non- consumer users and administrators on all system components as follows:	**8.5** Review procedures and interview personnel to verify that procedures are implemented for user identification and authentication management, by performing the following:			
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**8.5.1** Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to policy by performing the following: ? Obtain and examine an authorization form for each ID. ? Verify that the sampled user IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained), by tracing information from the authorization form to the system.	N/A – Security policy and procedures (ID / Account Management) is the responsibility of the merchant / service provider. Creation of access request (authorization) forms for access to PCI “in scope” systems, including: firewalls, routers, switches, VPNs, AD domain access, servers, databases, and applications, is the responsibility of the merchant / service provider.		
8.5.2 Verify user identity before performing password resets.	**8.5.2** Examine password/authentication procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user’s identity is verified before the password is reset.	N/A – Security policy and procedures (ID / Account Management) is the responsibility of the merchant / service provider. Account management / password reset procedures are the responsibility of the merchant / service provider.		

8.5.3 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.	**8.5.3** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use.	N/A – Security policy and procedures (ID / Account Management) is the responsibility of the merchant / service provider. Account management / password reset procedures are the responsibility of the merchant / service provider.		
8.5.4 Immediately revoke access for any terminated users.	**8.5.4** Select a sample of users terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.	N/A – Processes to ensure prompt revocation of granted access rights and deletion / disabling of user IDs is the responsibility of the merchant / service provider.		

8.5.5 Remove/disable inactive user accounts at least every 90 days.	**8.5.5** Verify that inactive accounts over 90 days old are either removed or disabled.	N/A – Manual audit procedure or third party ID management tool is the responsibility of the merchant / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.	**8.5.6.a** Verify that any accounts used by vendors to access, support and maintain system components are disabled, and enabled only when needed by the vendor.	N/A – No external vendor accounts were identified during the assessment.		
	8.5.6.b Verify that vendor remote access accounts are monitored while being used.	N/A – No external vendor accounts were identified during the assessment.		
8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.	**8.5.7** Interview the users from a sample of user IDs, to verify that they are familiar with authentication procedures and policies.	N/A – Security Policy (Security Awareness) is the responsibility of the merchant / service provider.		

8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	**8.5.8.a** For a sample of system components, examine user ID lists to verify the following: Generic user IDs and accounts are disabled or removed Shared user IDs for system administration activities and other critical functions do not exist Shared and generic user IDs are not used to administer any system components	Verizon Business reviewed user ID lists for all PCI Reference Architecture for Retail Solution components and verified that generic or shared user IDs and accounts are not used. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	8.5.8.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.	N/A – Security Policy (Password policy/procedures) is the responsibility of the merchant / service provider.		.
	8.5.8.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.	N/A – Security Policy (Password policy/procedures) is the responsibility of the merchant / service provider.		.

8.5.9 Change user passwords at least every 90 days.	**8.5.9.a** For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to change user passwords at least every 90 days. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

	8.5.9.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to change periodically and that non- consumer users are given guidance as to when, and under what circumstances, passwords must change.	N/A – For the purpose of this assessment, Cisco is not a service provider.		

8.5.10 Require a minimum password length of at least seven characters.	**8.5.10.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to require a minimum password length of at least seven characters. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		UCS-SRE may require compensating controls

	8.5.10.b For service providers only, review internal processes and customer/user documentation to verify that that non-consumer user passwords are required to meet minimum length requirements.	N/A – For the purpose of this assessment, Cisco is not a service provider.		

8.5.11 Use passwords containing both numeric and alphabetic characters.	**8.5.11.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to use passwords containing both numeric and alphabetic characters. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

	8.5.11.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to contain both numeric and alphabetic characters.	N/A – For the purpose of this assessment, Cisco is not a service provider.		

8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	**8.5.12.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage SwitcheCisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

	8.5.12.b For service providers only, review internal processes and customer/user documentation to verify that new non-consumer user passwords cannot be the same as the previous four passwords.	N/A – For the purpose of this assessment, Cisco is not a service provider.		

8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**8.5.13.a** For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than six invalid logon attempts.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to limit repeated access attempts by locking out the user ID after not more than six attempts. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage SwitcheCisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

	8.5.13.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user accounts are temporarily locked-out after not more than six invalid access attempts.	N/A – For the purpose of this assessment, Cisco is not a service provider.		

8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	**8.5.14** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured to set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage SwitcheCisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		UCS-SRE may require compensating controls. For routers, switches, firewalls, you will need manual reviews to accomplish, or use an external AAA service such as TACACS or RADIUS which can perform this function for user accounts.

8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**8.5.15** For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.	Verizon Business reviewed configuration settings for authentication methods to verify that all PCI Reference Architecture for Retail Solutions are configured in such a way that If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage SwitcheCisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.	**8.5.16.a** Review database and application configuration settings and verify that all users are authenticated prior to access.	N/A – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the merchant / service provider.		
	8.5.16.b Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).	N/A – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the merchant / service provider.		
	8.5.16.c Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators.	N/A – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the merchant / service provider.		
	8.5.16.d Review database applications and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).	N/A – Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the merchant / service provider.		

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	**9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco Video Surveillance Cisco Physical Access Control		

9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. **Note:** "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.	**9.1.1.a** Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider. Verizon Business observed system-generated configuration output for the following system components: Video Surveillance Physical Access Control Manager		
	9.1.1.b Verify that video cameras and/or access control mechanisms are protected from tampering or disabling.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
	9.1.1.c Verify that video cameras and/or access control mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.1.2 Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.	**9.1.2** Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized onsite personnel. Alternatively, verify that visitors are escorted at all times in areas with active network jacks.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider. Verizon Business observed system-generated configuration output for the following system components: Cisco Identity Services Engine Cisco switches-store Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560E Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R Cisco Unified Communications Manager and IP Phones		

9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	**9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	**9.2.a** Review processes and procedures for assigning badges to onsite personnel and visitors, and verify these processes include the following: requirements, and Revoking terminated onsite personnel and expired visitor badges	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
	9.2.b Verify that access to the badge system is limited to authorized personnel.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
	9.2.c Examine badges in use to verify that they clearly identify visitors and it is easy to distinguish between onsite personnel and visitors.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.3 Make sure all visitors are handled as follows:	**9.3** Verify that visitor controls are in place as follows:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained.	**9.3.1** Observe the use of visitor ID badges to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		

9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.	**9.3.2.a** Observe people within the facility to verify the use of visitor ID badges, and that visitors are easily distinguishable from onsite personnel.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
	9.3.2.b Verify that visitor badges expire.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.	**9.3.3** Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	**9.4.a** Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
	9.4.b Verify that the log contains the visitor's name, the firm represented, and the onsite personnel authorizing physical access, and is retained for at least three months.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		

9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.	**9.5.a** Observe the storage location's physical security to confirm that backup media storage is secure.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
	9.5.b Verify that the storage location security is reviewed at least annually.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.6 Physically secure all media.	**9.6** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:	**9.7** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.7.1 Classify media so the sensitivity of the data can be determined.	**9.7.1** Verify that all media is classified so the sensitivity of the data can be determined.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.	**9.7.2** Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	**9.8** Select a recent sample of several days of offsite tracking logs for all media, and verify the presence in the logs of tracking details and proper management authorization.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		

9.9 Maintain strict control over the storage and accessibility of media.	**9.9** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	**9.9.1** Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.10 Destroy media when it is no longer needed for business or legal reasons as follows:	**9.10** Obtain and examine the periodic media destruction policy and verify that it covers all media, and confirm the following:	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	**9.10.1.a** Verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a “to-be-shredded” container has a lock preventing access to its contents.	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	**9.10.2** Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).	N/A – Security Policy/Procedures (Physical Security) is the responsibility of the merchant / service provider.		

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments

10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that audit trails are enabled and active on all PCI Reference Architecture for Retail Solutions. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews, examination of audit logs, and examination of audit log settings, perform the following:			

10.2.1 All individual accesses to cardholder data	**10.2.1** Verify all individual access to cardholder data is logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that all individual access to cardholder data is logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Verify actions taken by any individual with root or administrative privileges are logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that actions taken by any individual with root or administrative privileges are logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2.3 Access to all audit trails	**10.2.3** Verify access to all audit trails is logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that access to all audit trails is logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2.4 Invalid logical access attempts	**10.2.4** Verify invalid logical access attempts are logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that invalid logical access attempts are logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2 5 Use of identification and authentication mechanisms	**10.2.5** Verify use of identification and authentication mechanisms is logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that use of identification and authentication mechanisms is logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2.6 Initialization of the audit logs	**10.2.6** Verify initialization of audit logs is logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that initialization of audit logs is logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.2.7 Creation and deletion of system-level objects	**10.2.7** Verify creation and deletion of system level objects are logged.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that creation and deletion of system level objects are logged. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.3 Record at least the following audit trail entries for all system components for each event:	**10.3** Through interviews and observation, for each auditable event (from 10.2), perform the following:			

10.3.1 User identification	**10.3.1** Verify user identification is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that user identification is included in log entries. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.3.2 Type of event	**10.3.2** Verify type of event is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that type of event is included in log entries. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.3.3 Date and time	**10.3.3** Verify date and time stamp is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that date and time stamp is included in log entries. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.3.4 Success or failure indication	**10.3.4** Verify success or failure indication is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that success or failure indication is included in log entries. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.3.5 Origination of event	**10.3.5** Verify origination of event is included in log entries.	Verizon Business interviewed personnel, reviewed log configuration settings and audit trails of the PCI Reference Architecture for Retail Solutions to verify that origination of event is included in log entries. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Catalyst 6500 Series Intrusion Detection Services Module2 Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.3.6 Identity or name of affected data, system component, or resource.	**10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries.	Verizon Business interviewed personnel,		
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. **Note:** One example of time synchronization technology is Network Time Protocol (NTP).	**10.4.a** Verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that NTP is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.		
	10.4.b Obtain and review the process for acquiring, distributing and storing the correct time within the organization, and review the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:			

10.4.1 Critical systems have the correct and consistent time.	**10.4.1.a** Verify that only designated central time servers receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that only designated central time servers receive time signals from external sources, and time signals from external sources are based on universally accepted time. Verizon Business observed system-generated configuration output for the following system components: Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-store Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560E Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		

	10.4.1.b Verify that the designated central time servers peer with each other to keep accurate time, and other internal servers receive time only from the central time servers.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that the designated central time servers peer with each other to keep accurate time, and other internal servers receive time only from the central time servers. Verizon Business observed system-generated configuration output for the following system components: Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco switches-store Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560E Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		

10.4.2 Time data is protected.	**10.4.2.a** Review system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that access to time data is restricted to only personnel with a business need to access time data Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 MDS Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

	10.4.2.b Review system configurations and time synchronization settings and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that any changes to time settings on critical systems are logged, monitored, and reviewed. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision SSL VPN Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.4.3 Time settings are received from industry-accepted time sources.	**10.4.3** Verify that the time servers accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that the time servers accept time updates from specific, industry-accepted external sources. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.5 Secure audit trails so they cannot be altered.	**10.5** Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that audit trails are secured so that they cannot be altered as follows:		

10.5.1 Limit viewing of audit trails to those with a job-related need.	**10.5.1** Verify that only individuals who have a job-related need can view audit trail files.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that only individuals who have a job-related need can view audit trail files. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Video Surveillance Cisco Physical Access Control		

10.5.2 Protect audit trail files from unauthorized modifications.	**10.5.2** Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Video Surveillance Cisco Physical Access Control		

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that current audit trail files are promptly backed up to a centralized log server that is difficult to alter. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Virtual Service Gateway Cisco Firewall Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945 Cisco routers-data center Cisco ASR 1002 Cisco 7206 Cisco MDS Storage Switches Cisco switches-data center Cisco Catalyst 6509 Cisco Catalyst 4948 Cisco Nexus 7010 Cisco Nexus 5020 Cisco Security Manager (CSM) HyTrust Appliance Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E EMC Ionix Network Configuration Manager EMC CLARiiON CX-240 RSA Authentication Manager RSA Data Protection Manager RSA enVision Cisco Identity Services Engine Cisco Virtual Service Gateway Cisco UCS Express on Services Ready Engine Cisco Unified Communications Manager and IP Phones Cisco Unified Computing System (UCS) Cisco Secure Access Control Server Cisco Video Surveillance Cisco Physical Access Control		

10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	**10.5.4** Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that logs for external-facing technologies are sent to a secure centralized internal log server.		
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	**10.5.5** Verify the use of file-integrity monitoring or change- detection software for logs by examining system settings and monitored files and results from monitoring activities.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that use of file-integrity monitoring software for logs by examining system settings and monitored files and results from monitoring activities. Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Communications Manager and IP Phones Cisco Video Surveillance Cisco Physical Access Control Cisco Unified Computing System (UCS) RSA Authentication Manager Cisco Security Manager EMC Ionix Network Configuration Manager RSA Data Protection Manager Cisco MDS Storage Switches EMC CLARiiON CX-240 Cisco Secure Access Control Server	This requirement is met by the use of the RSA enVision server aggregating each of the device logs and file integrity monitoring being provided by the RSA enVision software.	
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). **Note:** Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.	**10.6.a** Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.	N/A – Policies and Procedures is the responsibility of the merchant / service provider.		
	10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components.	Verizon Business reviewed configuration settings of PCI Reference Architecture for Retail Solutions to verify that log aggregation solutions generate events and alerts which are reviewed daily.		

10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	**10.7.a** Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.	N/A – Security Policy (Data Retention) is the responsibility of the merchant / service provider.		
	10.7.b Verify that audit logs are available for at least one year and processes are in place to immediately restore at least the last three months' logs for analysis.	Verizon Business reviewed online logs and audit trail archive methods within the PCI Reference Architecture for Retail Solutions environment to confirm that audit trails can be retained for at least one year, with at least three months available online.		

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. **Note:** Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.	**11.1.a** Verify that the entity has a documented process to detect and identify wireless access points on a quarterly basis.	Verizon Business confirmed that wireless controllers are configured to continually scan and detect rogue APs and wireless devices.		

	11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: WLAN cards inserted into system components Portable wireless devices connected to system components (for example, by USB, etc.) Wireless devices attached to a network port or network device	Verizon Business verified that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: WLAN cards inserted into system components Portable wireless devices connected to system components (for example, by USB, etc.) Wireless devices attached to a network port or network device Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E Cisco Identity Services Engine Cisco switches-store Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560E Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		
	11.1.c Verify that the documented process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities.	N/A – Policy and procedures is the responsibility of the merchant / service provider.		

	11.1.d If automated monitoring is utilized (for example, wireless IDS/, NAC, etc.), verify the configuration will generate alerts to personnel.	Verizon Business verified If automated monitoring is utilized, the configuration will generate alerts to personnel. Verizon Business observed system-generated configuration output for the following system components: Cisco Unified Wireless AIR-CT5508 MSE3550 Cisco WCS Manager AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N Cisco Identity Services Engine Cisco switches-store Cisco Catalyst 2960 Cisco Catalyst 2960G Cisco Catalyst 2960PD Cisco Catalyst 2960CPD Cisco Catalyst 2960S Cisco Catalyst 3560E Cisco Catalyst 3560X Cisco Catalyst 3560CPD Cisco Catalyst 3750X Cisco Catalyst 4507+R		
	11.1.e Verify the organization’s incident response plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.		

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component Installations, changes in network topology, firewall rule modifications, product upgrades). **Note:** It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented	**11.2** Verify that internal and external vulnerability scans are performed as follows:			
11.2.1 Perform quarterly internal vulnerability scans.	**11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.	N/A – Internal quarterly scanning is the responsibility of the merchant / service provider.		
	11.2.1.b Review the scan reports and verify that the scan process includes rescans until passing results are obtained, or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.	N/A – Internal quarterly scanning is the responsibility of the merchant / service provider.		
	11.2.1.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA	N/A – Internal quarterly scanning is the responsibility of the merchant / service provider.		

11.2.2 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). **Note:** Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by internal staff.	**11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly scans occurred in the most recent 12-month period.	N/A – Third party external, quarterly scanning is the responsibility of the merchant / service provider.		
	11.2.2.b Review the results of each quarterly scan to ensure that they satisfy the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no	N/A – Third party external, quarterly scanning is the responsibility of the merchant / service provider.		
	11.2.2.c Review the scan reports to verify that the scans were completed by an Approved Scanning Vendor (ASV), approved by the PCI SSC.	N/A – Third party external, quarterly scanning is the responsibility of the merchant / service provider.		

11.2.3 Perform internal and external scans after any significant change. **Note:** Scans conducted after changes may be performed by internal staff.	**11.2.3.a** Inspect change control documentation and scan reports to verify that system components subject to any significant change were scanned.	N/A – Third party external scanning / Internal scanning is the responsibility of the merchant / service provider.		
	11.2.3.b Review scan reports and verify that the scan process includes rescans until: For external scans, no vulnerabilities exist that are scored greater than a 4.0 by the CVSS, For internal scans, a passing result is obtained or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.	N/A – Third party external scanning / Internal scanning is the responsibility of the merchant / service provider.		
	11.2.3.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	N/A – Third party external scanning / Internal scanning is the responsibility of the merchant / service provider.		

11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:	**11.3.a** Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment.	N/A – Penetration Testing is the responsibility of the merchant / service provider.		
	11.3.b Verify that noted exploitable vulnerabilities were corrected and testing repeated.	N/A – Penetration Testing is the responsibility of the merchant / service provider.		
	11.3.c Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not	N/A – Penetration Testing is the responsibility of the merchant / service provider.		
11.3.1 Network-layer penetration tests	**11.3.1** Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems.	N/A – Penetration Testing is the responsibility of the merchant / service provider.		
11.3.2 Application-layer penetration tests	**11.3.2** Verify that the penetration test includes application-layer penetration tests. The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.	N/A – Penetration Testing is the responsibility of the merchant / service provider.		

11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	**11.4.a** Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored.	Verizon Business reviewed all IDS/ within the PCI Reference Architecture for Retail Solutions environment and confirmed that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored. Verizon Business observed system-generated configuration output for the following system components: Cisco ASA 5500 Series-data center Cisco ASA 5585 Cisco ASA 5540 Cisco ASA 5500 Series-store Cisco ASA 5510 Cisco Intrusion Detection Services Module Cisco routers-store Cisco 891W Cisco 1941W Cisco 2921 Cisco 2951 Cisco 3945		
	11.4.b Confirm IDS and/or are configured to alert personnel of suspected compromises.	Verizon Business reviewed all IDS/ within the PCI Reference Architecture for Retail Solutions environment and confirmed that they are configured to alert personnel of suspected compromises.		
	11.4.c Examine IDS/ configurations and confirm IDS/ devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.	Verizon Business reviewed all IDS/ within the PCI Reference Architecture for Retail Solutions environment and confirmed that they are configured, maintained, and updated per vendor instructions to ensure optimal protection.		

11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. **Note:** For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).	**11.5.a** Verify the use of file-integrity monitoring tools within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: System executables Application executables Configuration and parameter files Centrally stored, historical or archived, log and audit files	Verizon Business reviewed FIM settings, monitored files, and results from monitoring activities within the PCI Reference Architecture for Retail Solutions environment and verified that file-integrity monitoring tools are used.		
	11.5.b Verify the tools are configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly.	Verizon Business reviewed FIM settings, monitored files, and results from monitoring activities within the PCI Reference Architecture for Retail Solutions environment and verified that FIM is to be configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly by the merchant or service provider.		

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).	N/A – Security Policy is the responsibility of the merchant / service provider.		
12.1.1 Addresses all PCI DSS requirements.	**12.1.1** Verify that the policy addresses all PCI DSS requirements.	N/A – Security Policy is the responsibility of the merchant / service provider.		
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.)	**12.1.2.a** Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.	N/A – Security Policy is the responsibility of the merchant / service provider.		
	12.1.2.b Review risk assessment documentation to verify that the risk assessment process is performed at least annually.	N/A – Security Policy is the responsibility of the merchant / service provider.		
12.1.3 Includes a review at least annually and updates when the environment changes.	**12.1.3** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.	N/A – Security Policy is the responsibility of the merchant / service provider.		

12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	**12.2** Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.	N/A – Security Policy and Procedures is the responsibility of the merchant / service provider.		
12.3 Develop usage policies for critical technologies (for example, remote- access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following:	**12.3** Obtain and examine the usage policies for critical technologies and perform the following:			
12.3.1 Explicit approval by authorized parties	**12.3.1** Verify that the usage policies require explicit approval from authorized parties to use the technologies.	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.		
12.3.2 Authentication for use of the technology	**12.3.2** Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (for example, token).	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.		
12.3.3 A list of all such devices and personnel with access	**12.3.3** Verify that the usage policies require a list of all devices and personnel authorized to use the devices.	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.		
12.3.4 Labeling of devices to determine owner, contact information and purpose	**12.3.4** Verify that the usage policies require labeling of devices with information that can be correlated to owner, contact information and purpose.	N/A – Acceptable Use Policy / Asset List is the responsibility of the merchant / service provider.		
12.3.5 Acceptable uses of the technology	**12.3.5** Verify that the usage policies require acceptable uses for the technology.	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.		
12.3.6 Acceptable network locations for the technologies	**12.3.6** Verify that the usage policies require acceptable network locations for the technology.	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.		

12.3.7 List of company-approved products	**12.3.7** Verify that the usage policies require a list of company- approved products.	N/A – Acceptable Use Policy is the responsibility of the merchant / service provider.		
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	**12.3.8** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	N/A – Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.		
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	**12.3.9** Verify that the usage policies require activation of remote- access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	N/A – Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.		
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	**12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	N/A – Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.		
	12.3.10.b For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.	N/A – Acceptable Use / Remote Access Policy is the responsibility of the merchant / service provider.		
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**12.4** Verify that information security policies clearly define information security responsibilities for all personnel.	N/A – Security Policy is the responsibility of the merchant / service provider.		
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:	N/A – Security Policy is the responsibility of the merchant / service provider.		

12.5.1 Establish, document, and distribute security policies and procedures.	**12.5.1** Verify that responsibility for creating and distributing security policies and procedures is formally assigned.	N/A – Security Policy is the responsibility of the merchant / service provider.		
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	**12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.	N/A – Security Policy (Risk / Vulnerability management) is the responsibility of the merchant / service provider.		
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**12.5.3** Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned.	N/A – Security Policy (Risk / Vulnerability management) is the responsibility of the merchant / service provider.		
12.5.4 Administer user accounts, including additions, deletions, and modifications	**12.5.4** Verify that responsibility for administering user account and authentication management is formally assigned.	N/A – Security Policy (ID / Account management) is the responsibility of the merchant / service provider.		
12.5.5 Monitor and control all access to data.	**12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned.	N/A – Security Policy (Data Control / Monitoring) is the responsibility of the merchant / service provider.		
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	**12.6.a** Verify the existence of a formal security awareness program for all personnel.	N/A – Security Policy (Security Awareness) is the responsibility of the merchant / service provider.		
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:			
12.6.1 Educate personnel upon hire and at least annually. **Note:** Methods can vary depending on the role of the personnel and their level of access to the cardholder data.	**12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions).	N/A – Security Policy (Security Awareness) is the responsibility of the merchant / service provider.		

	12.6.1.b Verify that personnel attend awareness training upon hire and at least annually.	N/A – Security Policy (Security Awareness) is the responsibility of the merchant / service provider.		
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	**12.6.2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.	N/A – Security Policy (Security Awareness) is the responsibility of the merchant / service provider.		
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) **Note:** For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	**12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential personnel prior to hire who will have access to cardholder data or the cardholder data environment.	N/A – Security Policy (Background Checks) is the responsibility of the merchant / service provider.		
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	**12.8** If the entity shares cardholder data with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observation, review of policies and procedures, and review of supporting documentation, perform the following:			
12.8.1 Maintain a list of service providers.	**12.8.1** Verify that a list of service providers is maintained.	N/A – Connected Entity List (List of Service Providers with whom cardholder data is shared) is the responsibility of the merchant / service provider.		

12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	**12.8.2** Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.	N/A – Third party contracts is the responsibility of the merchant / service provider.		
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**12.8.3** Verify that policies and procedures are documented and were followed including proper due diligence prior to engaging any service provider.	N/A – Policies and Procedures for sharing cardholder data with third parties / Service Providers is the responsibility of the merchant / service provider.		
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	**12.8.4** Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.	N/A – Policies and Procedures for sharing cardholder data with third parties / Service Providers is the responsibility of the merchant / service provider.		
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**12.9** Obtain and examine the Incident Response Plan and related procedures and perform the following:			
12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum Specific incident response procedures Business recovery and continuity procedures Data back-up processes Analysis of legal requirements for reporting compromises Coverage and responses of all critical system components Reference or inclusion of incident response procedures from the payment brands	**12.9.1.a** Verify that the incident response plan includes: -Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum: Specific incident response procedures Business recovery and continuity procedures Data back-up processes Analysis of legal requirements for reporting compromises (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database) Coverage and responses for all critical system components Reference or inclusion of incident response procedures from the payment brands	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.		

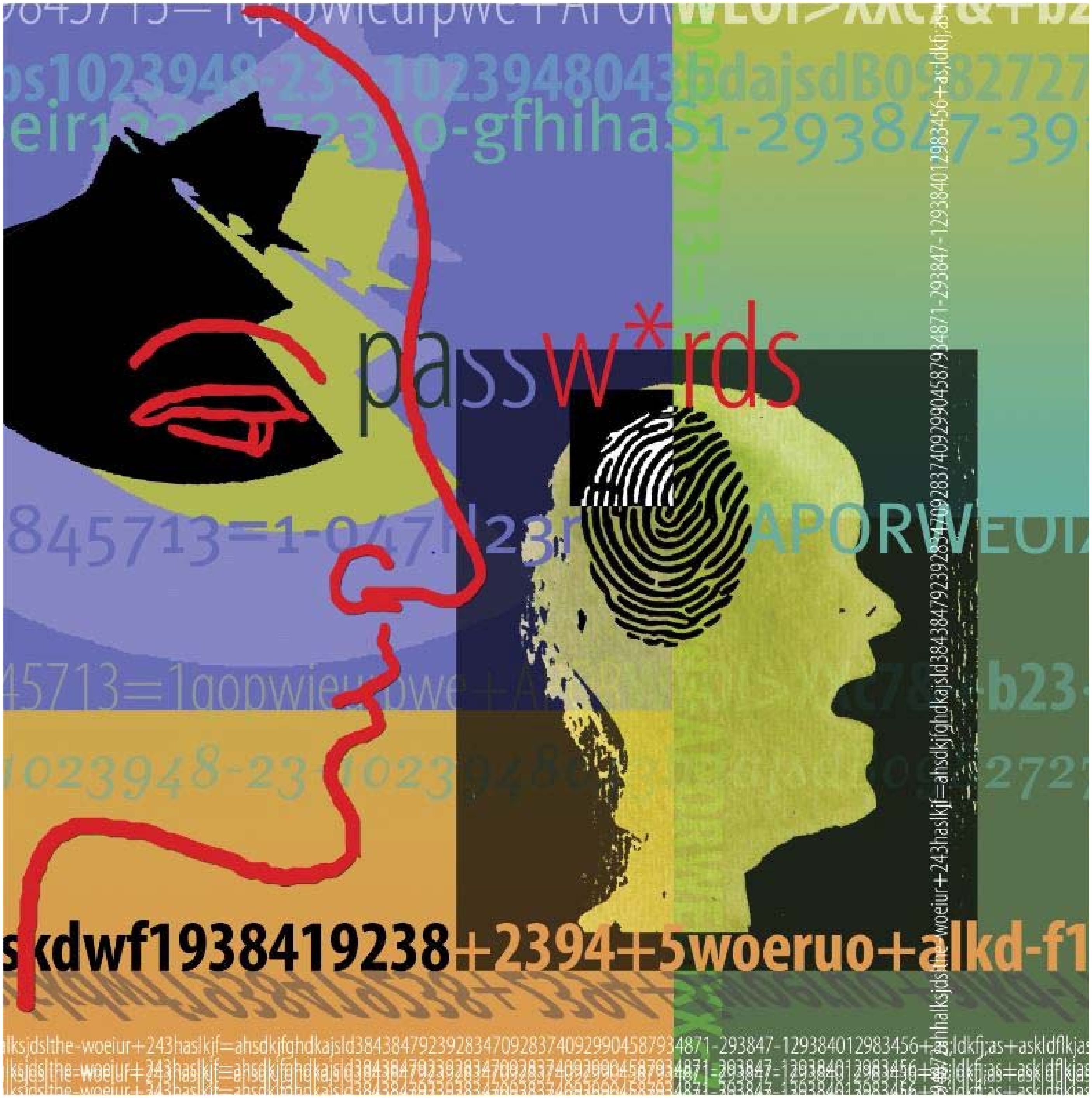
	12.9.1.b Review documentation from a previously reported incident or alert to verify that the documented incident response plan and procedures were followed.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.		
12.9.2 Test the plan at least annually.	**12.9.2** Verify that the plan is tested at least annually.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.		
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**12.9.3** Verify through observation and review of policies, that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.		
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	**12.9.4** Verify through observation and review of policies that staff with responsibilities for security breach response is periodically trained.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.		
12.9.5 Include alerts from intrusion- detection, intrusion-prevention, and file- integrity monitoring systems.	**12.9.5** Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.		
12.9.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**12.9.6** Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	N/A – Incident Response policy and procedures is the responsibility of the merchant / service provider.		

APPENDIX D

The Art of Compliance

Cisco's Global Retail Marketing team commissioned professional artists to create works of art inspired by PCI as a creative way to support Cisco's global launch of the Cisco PCI Solution for Retail 2.0. Each artist was given a description of the 12 requirements of PCI, general networking information, an overview of data security, and a description of Cisco's PCI solution. The following pages contain the artists' interpretations of the solution, networking, and data security.

To learn more, visit: www.cisco.com/go/pci2.


passw*rds
skdwf1938419238+2394+5woeruo+alkd-f1

Artist: Nancy Nimoy

Title: "Encrypted Data Crooks"

This piece is about encrypted data and the bad guys who steal it. When I thought of encrypted data, I thought of a human fingerprint and how it is literally a manifestation of what is inviolably unique about us. I thought to depict one's interior and deeply personal DNA. To communicate how our uniqueness is so often diminished and violated and "stolen" these days.

I used the universal symbol of theft, the generic black-cloaked burglar. He lurks behind the scrim of a loosely drawn human profile, encroaching upon the imperfect water color of a human head with its fingerprint brain. Layers of my piece are deliberately transparent and overlapping to convey "intrusion."

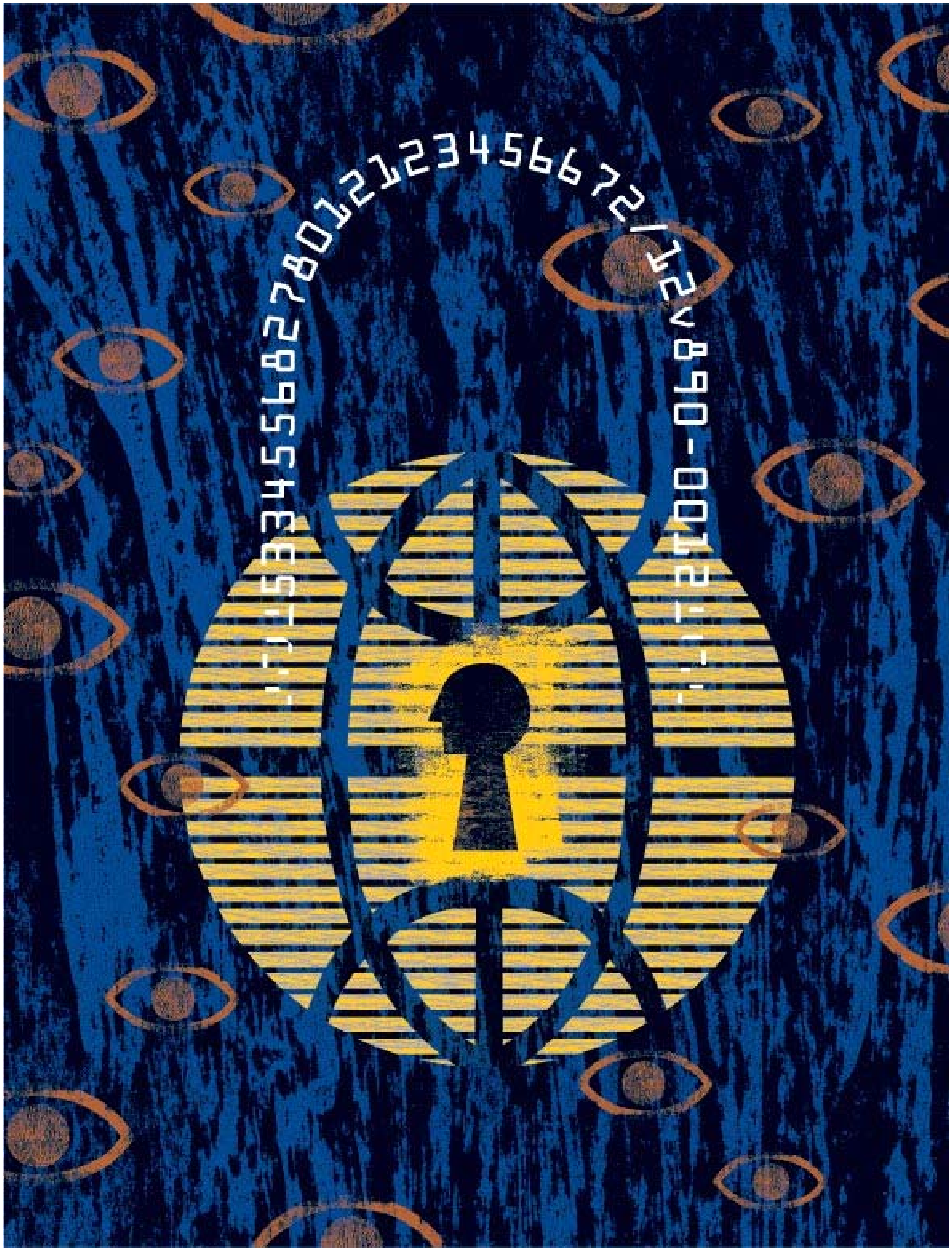
A cacophony of numbers, letters, codes, and secret passwords represent our pathetic defense against the onslaught of HTML bad guys trying to steal our encrypted data.

PCI
"INFORMATION LOCK DOWN"
Eric Thorsen

Artist: Eric Thorsen

Title: “Information Lock Down”

The credit card contained inside the lock illustrates how personal data can be withheld and protected from anyone not having the correct “key” or password. Restricting access to data with user IDs and passwords secures lock doors where sensitive data is stored.


11/1533455682278012123456672/12v890-0012

Artist: Matt Foster

Title: “Worldwide Data Safety”

Since the subject is technical in nature, this project needed subtlety and a connection to human elements. Since the image was planned for a myriad of viewing possibilities and would also be viewed worldwide, it needed to illustrate the complex, layered concept of the product yet be simple.

I started with a dark background, adding a layer of semi-transparent red eyes representing the checks and balances of the program, and also doubling as a “who else is looking” aspect. The lock is in the shape of the globe with the numbers being the security element. The keyhole is YOU- the user. The circle completes the world of secure data.

0360 8020 5609 4035
04/13

Artist: Lance Jackson

Title: “Stack”

A stack of credit cards is completely tantalizing eye candy. Credit cards are as American as apple pie and baseball. The bright pop-art colors are appropriately American. Knowing that the cards are secured wherever they are used is even more empowering.

P C I
LARRY JANOFF ©
"FAILED BREACH"

Artist: Larry Janoff

Title: “Failed Breach”

I was raised before the computer era, so conceptualizing a breach in security brings to my mind the “olden tools” used by a thief in the “olden days.” PCI is a difficult concept for people like me to comprehend, but the theme is SECURITY!

S. Averell

Artist: Sue Averell

Title: “Network Neighborhood”

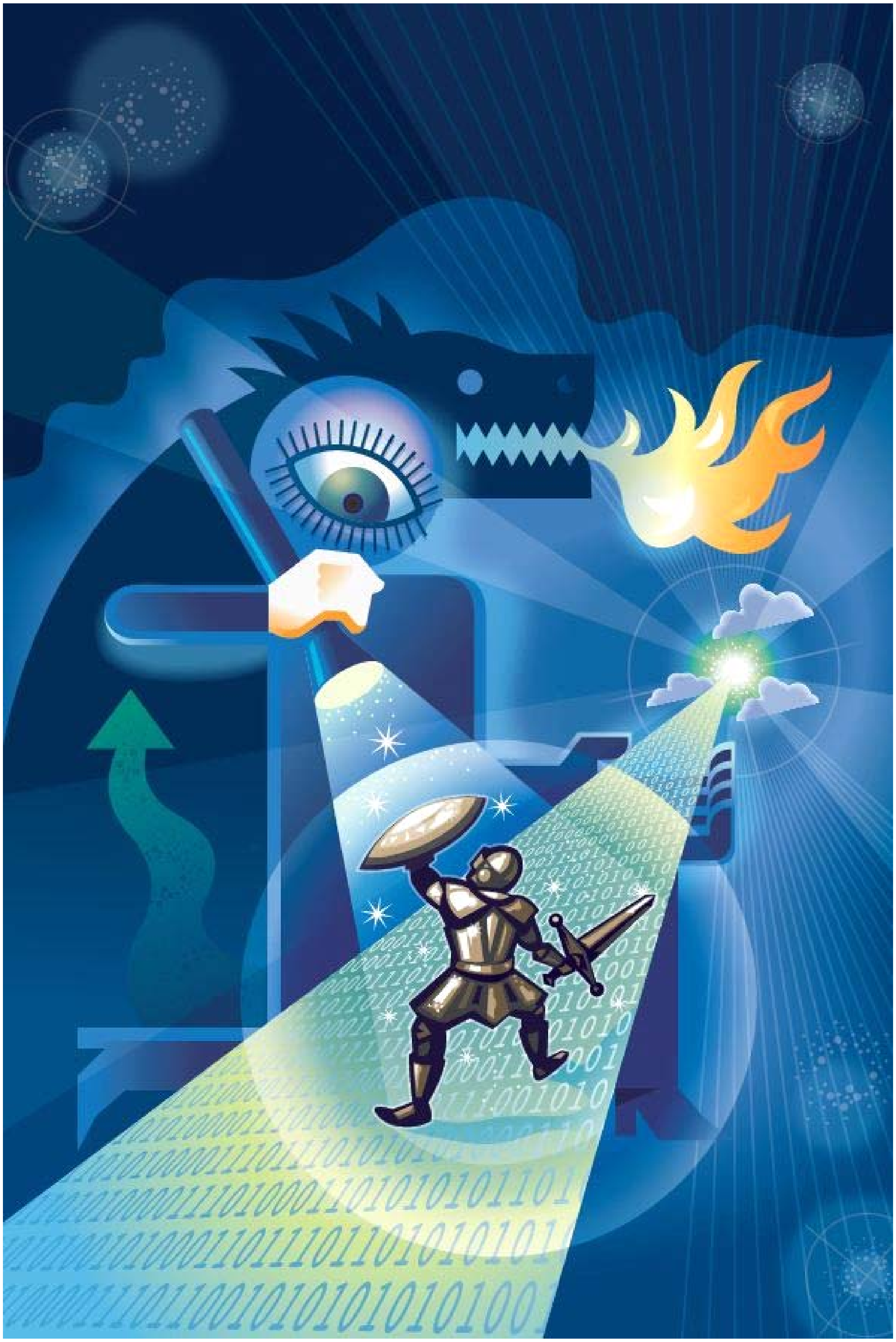
While creating this painting, I strove to combine my current theme of neighborhoods with that of data networks. It was important to me to be true to my style. Color and texture and an elevated view of the subject are some of the identifying characteristics of all my work.

PCI
"IMPENETRABLE FIREWALL"

Artist: Eric Thorsen

Title: “Impenetrable Firewall”

The sculpture of the fist attempting to break through the firewall, but being prevented from doing so, illustrates the basic strength of the essential software called a firewall. Personal computers and corporate computers alike require protection from predators, viruses, and software created to gather such data for ill purposes, including stealing money, data, or personal identities.



Artist: Filip Yip

Title: “Hacker”

Transferring private and important data over the Internet can expose users to the prying and hacking of ruthless cyber-criminals. There is an urgent need for a comprehensive solution to secure the safe transmission of information from point A to B. This godsend will be the cavalier who fights hackers incessantly, and strives to slay the dragon who has been devouring the most valuable and vulnerable asset of all netizens.

PCI
PCI
ADVANCED HACKING
CREDIT CARD NUMBERS
LARRY JANOFF ©
"THEY don't sleep at night"
Larry Janoff

Artist: Larry Janoff

Title: "THEY don't sleep at night"

I visualize a hacker as a vicious creature. I thought it humorous to represent him as a weird, evil monster that is trying very hard to breach PCI Security, someone who never sleeps, day or night.

Carte
1234 5678 9101 1213

Artist: Randy South

Title: "Secure Flight"

The objective of the work is to show that despite the dangers of maintaining financial security, freedom of commerce is still possible.

06/13

Artist: Lance Jackson

Title: “Secure Card”

Having your colorful, expressionistic, inner shopping self literally secured with chains and a lock says it all. You have the power to unlock it. No one else has that key.

PCI
PCI

Artist: Lance Jackson

Title: “Happy Network”

Shopping without information or a connection can be a dizzying, spinning experience. Why be sad or mad when you can be glad? By shopping on a secure networking you become a happy, smiling shopper. Being connected is the new shopping mantra.

PCI

Artist: Jerry Sprunger

Title: “Sanctuary”

The various components in this airbrushed painting serve to exhibit the security, service and reliability of Cisco’s PCI solution.

The credit cards and sensitive data behind the firewall on top of the rock pillar are secure due to the inaccessibility provided by two firewalls and secure pathways.The other globe-topped pillars in the background indicate the global coverage the systems offers. The bright light on the horizon is indicative of a bright, secure and strong future.

APPENDIX E

Detailed Full Running Configurations

This appendix includes the following device configurations:

ASA-DC-1

```
: Saved
:
ASA Version 8.4(1) <context>
!
firewall transparent
hostname dca-vc1
domain-name cisco-irn.com
enable password <removed> encrypted
passwd <removed> encrypted
names
!
interface outside
 nameif north
 bridge-group 1
 security-level 0
!
interface inside
 nameif south
 bridge-group 1
 security-level 100
!
interface BVI1
 ip address 192.168.162.21 255.255.255.0 standby 192.168.162.22
!
dns domain-lookup south
dns server-group DefaultDNS
 name-server 192.168.42.130
 domain-name cisco-irn.com
object-group network AdminStation
 network-object 192.168.41.101 255.255.255.255
object-group network AdminStation2
 network-object 192.168.41.102 255.255.255.255
object-group network AdminStation4-bart
 network-object 10.19.151.99 255.255.255.255
object-group network CSM_INLINE_src_rule_77309411633
 description Generated by CS-Manager from src of FirewallRule# 2
(ASA-DC-1-vdc1_v1/mandatory)
 group-object AdminStation
 group-object AdminStation2
 group-object AdminStation4-bart
object-group network DC-ALL
 description All of the Data Center
 network-object 192.168.0.0 255.255.0.0
object-group network Stores-ALL
 description all store networks
 network-object 10.10.0.0 255.255.0.0
object-group network CSM_INLINE_dst_rule_77309411633
 description Generated by CS-Manager from dst of FirewallRule# 2
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
object-group network EMC-NCM
 description EMC Network Configuration Manager
 network-object 192.168.42.122 255.255.255.255
object-group network CSManager
 description Cisco Security Manager
 network-object 192.168.42.133 255.255.255.255
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 network-object 192.168.42.124 255.255.255.255
object-group network AdminStation3
 network-object 192.168.42.138 255.255.255.255
object-group network Admin-Systems
 group-object EMC-NCM
 group-object AdminStation
 group-object AdminStation2
 group-object CSManager
 group-object RSA-enVision
 group-object AdminStation3
 group-object AdminStation4-bart
object-group network DC-DMZ
 description (Optimized by CS-Manager)
 network-object 192.168.20.0 255.255.252.0
 network-object 192.168.24.0 255.255.255.0
object-group network CSM_INLINE_dst_rule_77309411635
 description Generated by CS-Manager from dst of FirewallRule# 3
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
 group-object DC-DMZ
object-group network CSM_INLINE_src_rule_77309414079
 description Generated by CS-Manager from src of FirewallRule# 4
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
object-group network CSM_INLINE_src_rule_77309414081
 description Generated by CS-Manager from src of FirewallRule# 5
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
object-group network ActiveDirectory.cisco-irn.com
 network-object 192.168.42.130 255.255.255.255
object-group network vSphere-1
 description vSphere server for Lab
 network-object 192.168.41.102 255.255.255.255
object-group network WCSManager
 description Wireless Manager
 network-object 192.168.43.135 255.255.255.255
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for stores
 network-object 192.168.43.21 255.255.255.255
 network-object 192.168.43.22 255.255.255.255
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 network-object 192.168.43.31 255.255.255.255
 network-object 192.168.43.32 255.255.255.255
object-group network CSM_INLINE_src_rule_77309411641
 description Generated by CS-Manager from src of FirewallRule# 9
(ASA-DC-1-vdc1_v1/mandatory)
```

```
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
object-group network PAME-DC-1
 network-object 192.168.44.111 255.255.255.255
object-group network MSP-DC-1
 description Data Center VSOM
 network-object 192.168.44.121 255.255.255.255
object-group network CSM_INLINE_src_rule_77309411643
 description Generated by CS-Manager from src of FirewallRule# 10
(ASA-DC-1-vdc1_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
object-group network DC-WAAS
 description WAE Appliances in Data Center
 network-object 192.168.48.10 255.255.255.255
 network-object 192.168.49.10 255.255.255.255
 network-object 192.168.47.11 255.255.255.255
 network-object 192.168.47.12 255.255.255.255
object-group network CSM_INLINE_src_rule_77309414071
 description Generated by CS-Manager from src of FirewallRule# 15
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
object-group network NTP-Servers
 description NTP Servers
 network-object 192.168.62.161 255.255.255.255
 network-object 162.168.62.162 255.255.255.255
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 network-object 192.168.42.131 255.255.255.255
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 network-object 192.168.42.137 255.255.255.255
object-group network NAC-2
 network-object 192.168.42.112 255.255.255.255
object-group network NAC-1
 description ISE server for NAC
 network-object 192.168.42.111 255.255.255.255
object-group network CSM_INLINE_dst_rule_77309411663
 description Generated by CS-Manager from dst of FirewallRule# 25
(ASA-DC-1-vdc1_v1/mandatory)
 group-object TACACS
 group-object RSA-AM
 group-object NAC-2
 group-object NAC-1
object-group network CSM_INLINE_dst_rule_77309411665
 description Generated by CS-Manager from dst of FirewallRule# 26
(ASA-DC-1-vdc1_v1/mandatory)
 group-object NAC-2
 group-object NAC-1
object-group network CSM_INLINE_dst_rule_77309411669
 description Generated by CS-Manager from dst of FirewallRule# 28
(ASA-DC-1-vdc1_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
object-group network CSM_INLINE_dst_rule_77309411671
 description Generated by CS-Manager from dst of FirewallRule# 29
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
object-group network MS-Update
 description Windows Update Server
 network-object 192.168.42.150 255.255.255.255
```

```
object-group network MSExchange
 description Mail Server
 network-object 192.168.42.140 255.255.255.255
object-group network POS-Store-Conv
 network-object 10.10.160.81 255.255.255.255
object-group network POS-Store-MSP
 network-object 10.10.176.81 255.255.255.255
object-group network POS-Store-SMALL-1
 description Small Store POS devices
 network-object 10.10.128.81 255.255.255.255
 network-object 10.10.128.82 255.255.255.255
object-group network POS-Store-Medium
 network-object 10.10.112.81 255.255.255.255
 network-object 10.10.125.40 255.255.255.255
object-group network POS-Store-Mini
 network-object 10.10.144.81 255.255.255.255
object-group network POS-Store-3g
 network-object 10.10.192.82 255.255.255.255
object-group network POS-Store-Large
 network-object 10.10.96.81 255.255.255.255
 network-object 10.10.96.82 255.255.255.255
object-group network CSM_INLINE_src_rule_77309411683
 description Generated by CS-Manager from src of FirewallRule# 35
(ASA-DC-1-vdc1_v1/mandatory)
 group-object POS-Store-Conv
 group-object POS-Store-MSP
 group-object POS-Store-SMALL-1
 group-object POS-Store-Medium
 group-object POS-Store-Mini
 group-object POS-Store-3g
 group-object POS-Store-Large
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 network-object 192.168.52.96 255.255.255.224
object-group network DC-POS
 description POS in the Data Center
 network-object 192.168.52.0 255.255.255.0
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 network-object 192.168.52.144 255.255.255.240
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 network-object 192.168.52.128 255.255.255.240
object-group network CSM_INLINE_dst_rule_77309411683
 description Generated by CS-Manager from dst of FirewallRule# 35
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-POS-Tomax
 group-object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
object-group network CSM_INLINE_src_rule_77309414158
 description Generated by CS-Manager from src of FirewallRule# 36
(ASA-DC-1-vdc1_v1/mandatory)
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
 network-object 192.168.21.0 255.255.255.0
object-group network CSM_INLINE_src_rule_77309414160
 description Generated by CS-Manager from src of FirewallRule# 37
(ASA-DC-1-vdc1_v1/mandatory)
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
 network-object 192.168.21.0 255.255.255.0
object-group network CSM_INLINE_src_rule_77309414162
```

```
 description Generated by CS-Manager from src of FirewallRule# 38
(ASA-DC-1-vdc1_v1/mandatory)
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
 network-object 192.168.21.0 255.255.255.0
object-group service HTTPS-8443
 service-object tcp destination eq 8443
object-group service CSM_INLINE_svc_rule_77309411635
 description Generated by CS-Manager from service of FirewallRule# 3
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq ssh
 service-object tcp destination eq https
 group-object HTTPS-8443
object-group service CSM_INLINE_svc_rule_77309414079
 description Generated by CS-Manager from service of FirewallRule# 4
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq smtp
 service-object tcp destination eq https
 service-object tcp destination eq ssh
object-group service CSM_INLINE_svc_rule_77309414081
 description Generated by CS-Manager from service of FirewallRule# 5
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq ssh
object-group service RPC
 service-object tcp destination eq 135
object-group service LDAP-GC
 service-object tcp destination eq 3268
object-group service LDAP-GC-SSL
 service-object tcp destination eq 3269
object-group service DNS-Resolving
 description Domain Name Server
 service-object tcp destination eq domain
 service-object udp destination eq domain
object-group service Kerberos-TCP
 service-object tcp destination eq 88
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 service-object tcp destination eq 445
object-group service LDAP-UDP
 service-object udp destination eq 389
object-group service RPC-HighPorts
 service-object tcp destination range 1024 65535
object-group service CSM_INLINE_svc_rule_77309411637
 description Generated by CS-Manager from service of FirewallRule# 7
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq ntp
 service-object udp destination eq netbios-dgm
 group-object RPC
 group-object LDAP-GC
 group-object LDAP-GC-SSL
 group-object DNS-Resolving
 group-object Kerberos-TCP
 group-object Microsoft-DS-SMB
 group-object LDAP-UDP
 group-object RPC-HighPorts
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 service-object tcp destination eq 5989
 service-object tcp destination eq 8000
 service-object tcp destination eq 902
 service-object tcp destination eq 903
object-group service CSM_INLINE_svc_rule_77309411639
 description Generated by CS-Manager from service of FirewallRule# 8
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 group-object vCenter-to-ESX4
object-group service IP-Protocol-97
 description IP protocol 97
 service-object 97
object-group service TFTP
 description Trivial File Transfer
 service-object tcp destination eq 69
 service-object udp destination eq tftp
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 service-object udp destination eq 12222
 service-object udp destination eq 12223
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 service-object udp destination eq 5246
 service-object udp destination eq 5247
object-group service CSM_INLINE_svc_rule_77309411641
 description Generated by CS-Manager from service of FirewallRule# 9
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq www
 service-object udp destination eq isakmp
 service-object tcp destination eq telnet
 service-object tcp destination eq ssh
 group-object IP-Protocol-97
 group-object TFTP
 group-object LWAPP
 group-object CAPWAP
object-group service TCP1080
 service-object tcp destination eq 1080
object-group service TCP8080
 service-object tcp destination eq 8080
object-group service RDP
 description Windows Remote Desktop
 service-object tcp destination eq 3389
object-group service CSM_INLINE_svc_rule_77309411645
 description Generated by CS-Manager from service of FirewallRule# 11
(ASA-DC-1-vdc1_v1/mandatory)
 service-object icmp echo
 service-object icmp echo-reply
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object tcp destination eq ftp
 group-object HTTPS-8443
 group-object TCP1080
 group-object TCP8080
 group-object RDP
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 service-object tcp destination eq 4050
object-group service Netbios
 description Netbios Servers
 service-object udp destination eq netbios-dgm
 service-object udp destination eq netbios-ns
 service-object tcp destination eq netbios-ssn
object-group service CSM_INLINE_svc_rule_77309411647
```

```
 description Generated by CS-Manager from service of FirewallRule# 12 
(ASA-DC-1-vdc1_v1/mandatory)
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
 group-object Netbios
object-group service CSM_INLINE_svc_rule_77309411649
 description Generated by CS-Manager from service of FirewallRule# 13 
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group service CSM_INLINE_svc_rule_77309414071
 description Generated by CS-Manager from service of FirewallRule# 15 
(ASA-DC-1-vdc1_v1/mandatory)
 service-object icmp echo
 service-object icmp echo-reply
 service-object icmp unreachable
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ftp
 service-object tcp destination eq ssh
 group-object TCP1080
 group-object TCP8080
 group-object RDP
object-group service NTP
 description NTP Protocols
 service-object tcp destination eq 123
 service-object udp destination eq ntp
object-group service CSM_INLINE_svc_rule_77309414073
 description Generated by CS-Manager from service of FirewallRule# 16 
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DNS-Resolving
 group-object NTP
object-group service CSM_INLINE_svc_rule_77309414077
 description Generated by CS-Manager from service of FirewallRule# 18 
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 group-object LDAP-GC
 group-object LDAP-GC-SSL
 group-object LDAP-UDP
object-group service CSM_INLINE_svc_rule_77309411655
 description Generated by CS-Manager from service of FirewallRule# 21 
(ASA-DC-1-vdc1_v1/mandatory)
 service-object udp destination eq snmptrap
 service-object udp destination eq snmp
 service-object udp destination eq syslog
object-group service CSM_INLINE_svc_rule_77309411657
 description Generated by CS-Manager from service of FirewallRule# 22 
(ASA-DC-1-vdc1_v1/mandatory)
 service-object udp destination eq domain
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
object-group service CSM_INLINE_svc_rule_77309411663
 description Generated by CS-Manager from service of FirewallRule# 25 
(ASA-DC-1-vdc1_v1/mandatory)
 service-object udp destination eq 1812
 service-object udp destination eq 1813
object-group service CSM_INLINE_svc_rule_77309411665
 description Generated by CS-Manager from service of FirewallRule# 26 
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq www
 group-object HTTPS-8443
```

```
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 service-object udp destination eq 427
 service-object tcp destination eq 427
object-group service CSM_INLINE_svc_rule_77309411667
 description Generated by CS-Manager from service of FirewallRule# 27
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq www
 service-object tcp destination eq ssh
 group-object vCenter-to-ESX4
 group-object ESX-SLP
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 service-object udp destination eq 16666
 service-object udp destination eq 16667
object-group service CSM_INLINE_svc_rule_77309411671
 description Generated by CS-Manager from service of FirewallRule# 29
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq https
 service-object udp destination eq isakmp
 group-object Cisco-Mobility
 group-object IP-Protocol-97
 group-object LWAPP
 group-object CAPWAP
object-group service CSM_INLINE_svc_rule_77309411673
 description Generated by CS-Manager from service of FirewallRule# 30
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group service CSM_INLINE_svc_rule_77309411675
 description Generated by CS-Manager from service of FirewallRule# 31
(ASA-DC-1-vdc1_v1/mandatory)
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
 group-object Netbios
object-group service CSM_INLINE_svc_rule_77309411677
 description Generated by CS-Manager from service of FirewallRule# 32
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq ntp
 service-object udp destination eq netbios-dgm
 group-object RPC
 group-object LDAP-GC
 group-object LDAP-GC-SSL
 group-object DNS-Resolving
 group-object Kerberos-TCP
 group-object Microsoft-DS-SMB
 group-object LDAP-UDP
 group-object RPC-HighPorts
object-group service CSM_INLINE_svc_rule_77309411679
 description Generated by CS-Manager from service of FirewallRule# 33
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq www
 service-object tcp destination eq https
object-group service CSM_INLINE_svc_rule_77309411681
 description Generated by CS-Manager from service of FirewallRule# 34
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq smtp
 service-object tcp destination eq pop3
 service-object tcp destination eq imap4
object-group service CSM_INLINE_svc_rule_77309414166
 description Generated by CS-Manager from service of FirewallRule# 40
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq smtp
 group-object DNS-Resolving
object-group service CSM_INLINE_svc_rule_77309414172
 description Generated by CS-Manager from service of FirewallRule# 43
(ASA-DC-1-vdc1_v1/mandatory)
 service-object udp destination eq 1812
 service-object udp destination eq 1813
object-group service CSM_INLINE_svc_rule_77309414176
 description Generated by CS-Manager from service of FirewallRule# 45
(ASA-DC-1-vdc1_v1/mandatory)
 service-object icmp
 service-object tcp destination eq ssh
 service-object tcp destination eq telnet
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq 8880
 service-object tcp destination eq 8444
 service-object tcp destination eq 5900
 service-object tcp destination eq 5800
 group-object RDP
 group-object TCP1080
 group-object TCP8080
 group-object TFTP
 group-object HTTPS-8443
 group-object vCenter-to-ESX4
access-list CSM_FW_ACL_north extended permit ospf 192.168.162.0 255.255.255.0
192.168.162.0 255.255.255.0
access-list CSM_FW_ACL_north extended permit tcp object-group Stores-ALL object-group
EMC-NCM eq ssh
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411655
object-group Stores-ALL object-group RSA-enVision
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411657
object-group Stores-ALL object-group ActiveDirectory.cisco-irn.com
access-list CSM_FW_ACL_north extended permit tcp object-group Stores-ALL object-group
TACACS eq tacacs
access-list CSM_FW_ACL_north extended permit udp object-group Stores-ALL object-group
NTP-Servers eq ntp
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411663
object-group Stores-ALL object-group CSM_INLINE_dst_rule_77309411663
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411665
object-group Stores-ALL object-group CSM_INLINE_dst_rule_77309411665
access-list CSM_FW_ACL_north remark VMWare ESX to Data Center
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411667
object-group Stores-ALL object-group vSphere-1
access-list CSM_FW_ACL_north remark Physical security systems
access-list CSM_FW_ACL_north extended permit tcp object-group Stores-ALL object-group
CSM_INLINE_dst_rule_77309411669 eq https
access-list CSM_FW_ACL_north remark Wireless control systems
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411671
object-group Stores-ALL object-group CSM_INLINE_dst_rule_77309411671
access-list CSM_FW_ACL_north remark Voice calls
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411673
object-group Stores-ALL object-group DC-ALL
access-list CSM_FW_ACL_north remark WAAS systems
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411675
object-group Stores-ALL object-group DC-WAAS
access-list CSM_FW_ACL_north remark Allow Active Directory Domain
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411677
object-group Stores-ALL object-group ActiveDirectory.cisco-irn.com
```

```
access-list CSM_FW_ACL_north remark Allow Windows Updates
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411679
object-group Stores-ALL object-group MS-Update
access-list CSM_FW_ACL_north remark Allow Mail
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411681
object-group Stores-ALL object-group MSExchange
access-list CSM_FW_ACL_north remark Allow Applications
access-list CSM_FW_ACL_north extended permit tcp object-group
CSM_INLINE_src_rule_77309411683 object-group CSM_INLINE_dst_rule_77309411683 eq https
access-list CSM_FW_ACL_north extended permit udp object-group
CSM_INLINE_src_rule_77309414158 object-group NTP-Servers eq ntp
access-list CSM_FW_ACL_north remark - RIE-2
access-list CSM_FW_ACL_north extended permit udp object-group
CSM_INLINE_src_rule_77309414160 object-group RSA-enVision eq syslog
access-list CSM_FW_ACL_north extended permit tcp object-group
CSM_INLINE_src_rule_77309414162 object-group TACACS eq tacacs
access-list CSM_FW_ACL_north extended permit udp 192.168.21.0 255.255.255.0 object-group
ActiveDirectory.cisco-irn.com eq domain
access-list CSM_FW_ACL_north remark Ironport traffic in from DNZ
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309414166
host 192.168.23.68 any
access-list CSM_FW_ACL_north extended permit udp host 192.168.23.68 object-group
RSA-enVision eq syslog
access-list CSM_FW_ACL_north extended permit udp host 192.168.23.68 object-group
NTP-Servers eq ntp
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309414172
host 192.168.23.68 object-group TACACS
access-list CSM_FW_ACL_north remark Drop all other traffic
access-list CSM_FW_ACL_north extended deny ip any any log
access-list CSM_FW_ACL_south extended permit ospf 192.168.162.0 255.255.255.0
192.168.162.0 255.255.255.0
access-list CSM_FW_ACL_south extended permit ip object-group
CSM_INLINE_src_rule_77309411633 object-group CSM_INLINE_dst_rule_77309411633
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411635
object-group Admin-Systems object-group CSM_INLINE_dst_rule_77309411635
access-list CSM_FW_ACL_south remark Allow services for Ironport apps
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309414079
object-group CSM_INLINE_src_rule_77309414079 192.168.23.64 255.255.255.224
access-list CSM_FW_ACL_south remark Allow traffic to DMZ
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309414081
object-group CSM_INLINE_src_rule_77309414081 host 192.168.20.30
access-list CSM_FW_ACL_south remark Drop unauthorized traffic to DMZ
access-list CSM_FW_ACL_south extended deny ip any 192.168.20.0 255.255.252.0 log
access-list CSM_FW_ACL_south remark Allow Active Directory Domain
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411637
object-group ActiveDirectory.cisco-irn.com object-group Stores-ALL
access-list CSM_FW_ACL_south remark VMWare - ESX systems
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411639
object-group vSphere-1 object-group Stores-ALL
access-list CSM_FW_ACL_south remark Wireless Management to Stores
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411641
object-group CSM_INLINE_src_rule_77309411641 object-group Stores-ALL
access-list CSM_FW_ACL_south remark Physical security systems
access-list CSM_FW_ACL_south extended permit tcp object-group
CSM_INLINE_src_rule_77309411643 object-group Stores-ALL eq https
access-list CSM_FW_ACL_south remark Allow Management of store systems
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411645
object-group DC-ALL object-group Stores-ALL
access-list CSM_FW_ACL_south remark WAAS systems
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411647
object-group DC-WAAS object-group Stores-ALL
access-list CSM_FW_ACL_south remark Voice calls
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411649
object-group DC-ALL object-group Stores-ALL
```

```
access-list CSM_FW_ACL_south extended deny ip any object-group Stores-ALL
access-list CSM_FW_ACL_south remark Allow outbound services for Internet
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309414071
object-group CSM_INLINE_src_rule_77309414071 any
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309414073
object-group ActiveDirectory.cisco-irn.com any
access-list CSM_FW_ACL_south extended permit udp object-group NTP-Servers any eq ntp
access-list CSM_FW_ACL_south remark Allow LDAP out LAB test
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309414077
object-group PAME-DC-1 any log
access-list CSM_FW_ACL_south remark Drop and Log all other traffic
access-list CSM_FW_ACL_south extended deny ip any any log
pager lines 24
logging host south 192.168.42.124
mtu north 1500
mtu south 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any north
icmp permit any south
asdm history enable
arp timeout 14400
access-group CSM_FW_ACL_north in interface north
access-group CSM_FW_ACL_south in interface south
route north 0.0.0.0 0.0.0.0 192.168.162.1 1
route south 192.168.38.0 255.255.255.0 192.168.162.7 1
route south 192.168.39.0 255.255.255.0 192.168.162.7 1
route south 192.168.40.0 255.255.255.0 192.168.162.7 1
route south 192.168.41.0 255.255.255.0 192.168.162.7 1
route south 192.168.42.0 255.255.255.0 192.168.162.7 1
route south 192.168.43.0 255.255.255.0 192.168.162.7 1
route south 192.168.44.0 255.255.255.0 192.168.162.7 1
route south 192.168.45.0 255.255.255.0 192.168.162.7 1
route south 192.168.46.0 255.255.255.0 192.168.162.7 1
route south 192.168.52.0 255.255.255.0 192.168.162.7 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (south) host 192.168.42.131
 key *****
aaa authentication ssh console RETAIL LOCAL
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa accounting ssh console RETAIL
aaa accounting enable console RETAIL
aaa accounting command privilege 15 RETAIL
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
http server enable
http server idle-timeout 15
http server session-timeout 60
http 10.19.151.99 255.255.255.255 north
http 192.168.41.101 255.255.255.255 south
http 192.168.41.102 255.255.255.255 south
http 192.168.42.122 255.255.255.255 south
http 192.168.42.124 255.255.255.255 south
http 192.168.42.133 255.255.255.255 south
http 192.168.42.138 255.255.255.255 south
no snmp-server location
no snmp-server contact
```

```
telnet timeout 5
ssh 10.19.151.99 255.255.255.255 north
ssh 192.168.41.101 255.255.255.255 south
ssh 192.168.41.102 255.255.255.255 south
ssh 192.168.42.122 255.255.255.255 south
ssh 192.168.42.124 255.255.255.255 south
ssh 192.168.42.133 255.255.255.255 south
ssh 192.168.42.138 255.255.255.255 south
ssh timeout 15
ssh version 2
no threat-detection statistics tcp-intercept
username csmadmin password  <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:70afa3a2a3007db41f3f336aca5cf51d
: end
asdm history enable
```

ASA-IE-1

```
: Saved
: Written by retail at 20:28:46.793 PDT Fri Apr 29 2011
!
ASA Version 8.4(1)
!
hostname ASA-IE-1
domain-name cisco-irn.com
enable password <removed> encrypted
passwd <removed> encrypted
names
dns-guard
!
```

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.21.1 255.255.255.0 standby 192.168.21.2
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.11.60 255.255.255.0 standby 192.168.11.62
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 description LAN/STATE Failover Interface
!
interface Management0/0
 no nameif
 no security-level
 no ip address
 management-only
!
boot system disk0:/asa841-k8.bin
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns domain-lookup outside
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 192.168.42.130
 domain-name cisco-irn.com
same-security-traffic permit inter-interface
object network AdminStation
 host 192.168.41.101
object network AdminStation2
 host 192.168.41.102
object network EMC-NCM
 host 192.168.42.122
 description EMC Network Configuration Manager
object network CSManager
 host 192.168.42.133
 description Cisco Security Manager
object network RSA-enVision
 host 192.168.42.124
 description RSA EnVision Syslog collector and SIM
object network AdminStation3
 host 192.168.42.138
object network AdminStation4-bart
 host 10.19.151.99
object network DC-ALL
 subnet 192.168.0.0 255.255.0.0
 description All of the Data Center
object network Stores-ALL
 subnet 10.10.0.0 255.255.0.0
 description all store networks
object network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
object network PAME-DC-1
 host 192.168.44.111
object network TACACS
 host 192.168.42.131
 description Csico Secure ACS server for TACACS and Radius
object service TCP1080
 service tcp destination eq 1080
object service TCP8080
 service tcp destination eq 8080
object service RDP
 service tcp destination eq 3389
 description Windows Remote Desktop
object service LDAP-GC
 service tcp destination eq 3268
object service LDAP-GC-SSL
 service tcp destination eq 3269
object service LDAP-UDP
 service udp destination eq 389
object-group network CSM_INLINE_src_rule_77309412132
 description Generated by CS-Manager from src of FirewallRule# 3 (ASA-IE-1_v1/mandatory)
 network-object object EMC-NCM
 network-object object AdminStation
 network-object object CSManager
 network-object object AdminStation2
 network-object object RSA-enVision
 network-object object AdminStation3
 network-object object AdminStation4-bart
object-group network CSM_INLINE_src_rule_77309412156
 description Generated by CS-Manager from src of FirewallRule# 4 (ASA-IE-1_v1/mandatory)
 network-object object DC-ALL
 network-object object Stores-ALL
object-group network CSM_INLINE_src_rule_77309412168
 description Generated by CS-Manager from src of FirewallRule# 5 (ASA-IE-1_v1/mandatory)
 network-object object DC-ALL
 network-object object Stores-ALL
object-group network CSM_INLINE_src_rule_77309412178
 description Generated by CS-Manager from src of FirewallRule# 7 (ASA-IE-1_v1/mandatory)
 network-object object DC-ALL
 network-object object Stores-ALL
object-group network NTP-Servers
 description NTP Servers
 network-object 192.168.62.161 255.255.255.255
 network-object 162.168.62.162 255.255.255.255
object-group network CSM_INLINE_src_rule_77309412254
 description Generated by CS-Manager from src of FirewallRule# 15 (ASA-IE-1_v1/mandatory)
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
 network-object 192.168.21.0 255.255.255.0
object-group network CSM_INLINE_src_rule_77309412258
 description Generated by CS-Manager from src of FirewallRule# 16 (ASA-IE-1_v1/mandatory)
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
 network-object 192.168.21.0 255.255.255.0
object-group network CSM_INLINE_src_rule_77309412260
 description Generated by CS-Manager from src of FirewallRule# 17 (ASA-IE-1_v1/mandatory)
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
 network-object 192.168.21.0 255.255.255.0
object-group service CSM_INLINE_svc_rule_77309412132
 description Generated by CS-Manager from service of FirewallRule# 3
(ASA-IE-1_v1/mandatory)
 service-object tcp destination eq ssh
 service-object tcp destination eq https
object-group service CSM_INLINE_svc_rule_77309412156
 description Generated by CS-Manager from service of FirewallRule# 4
(ASA-IE-1_v1/mandatory)
 service-object tcp destination eq smtp
 service-object tcp destination eq https
 service-object tcp destination eq ssh
object-group service CSM_INLINE_svc_rule_77309412168
 description Generated by CS-Manager from service of FirewallRule# 5
(ASA-IE-1_v1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq ssh
object-group service CSM_INLINE_svc_rule_77309412178
 description Generated by CS-Manager from service of FirewallRule# 7
(ASA-IE-1_v1/mandatory)
 service-object icmp echo
 service-object icmp echo-reply
 service-object icmp unreachable
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ftp
 service-object tcp destination eq ssh
 service-object object TCP1080
 service-object object TCP8080
 service-object object RDP
object-group service DNS-Resolving
 description Domain Name Server
 service-object tcp destination eq domain
 service-object udp destination eq domain
object-group service NTP
 description NTP Protocols
 service-object tcp destination eq 123
 service-object udp destination eq ntp
object-group service CSM_INLINE_svc_rule_77309412202
 description Generated by CS-Manager from service of FirewallRule# 8
(ASA-IE-1_v1/mandatory)
 group-object DNS-Resolving
 group-object NTP
object-group service CSM_INLINE_svc_rule_77309412216
 description Generated by CS-Manager from service of FirewallRule# 10
(ASA-IE-1_v1/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object object LDAP-GC
 service-object object LDAP-GC-SSL
 service-object object LDAP-UDP
object-group service TFTP
 description Trivial File Transfer
 service-object tcp destination eq 69
 service-object udp destination eq tftp
object-group service HTTPS-8443
 service-object tcp destination eq 8443
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 service-object tcp destination eq 5989
 service-object tcp destination eq 8000
 service-object tcp destination eq 902
 service-object tcp destination eq 903
object-group service CSM_INLINE_svc_rule_77309412222
 description Generated by CS-Manager from service of FirewallRule# 13
(ASA-IE-1_v1/mandatory)
 service-object icmp
 service-object tcp destination eq ssh
 service-object tcp destination eq telnet
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq 8880
 service-object tcp destination eq 8444
 service-object tcp destination eq 5900
 service-object tcp destination eq 5800
 service-object object RDP
 service-object object TCP1080
 service-object object TCP8080
 group-object TFTP
 group-object HTTPS-8443
 group-object vCenter-to-ESX4
object-group service CSM_INLINE_svc_rule_77309412276
 description Generated by CS-Manager from service of FirewallRule# 19
(ASA-IE-1_v1/mandatory)
 service-object tcp destination eq smtp
 group-object DNS-Resolving
object-group service CSM_INLINE_svc_rule_77309412288
 description Generated by CS-Manager from service of FirewallRule# 22
(ASA-IE-1_v1/mandatory)
 service-object udp destination eq 1812
 service-object udp destination eq 1813
access-list all extended permit ip any any
access-list INSIDE extended permit ip object AdminStation any
access-list INSIDE extended permit ip object AdminStation2 any
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_77309412132
object-group CSM_INLINE_src_rule_77309412132 192.168.20.0 255.255.252.0
access-list INSIDE remark Allow services for Ironport apps
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_77309412156
object-group CSM_INLINE_src_rule_77309412156 192.168.23.64 255.255.255.224
access-list INSIDE remark Allow traffic to DMZ
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_77309412168
object-group CSM_INLINE_src_rule_77309412168 host 192.168.20.30
access-list INSIDE remark Drop unauthorized traffic to DMZ
access-list INSIDE extended deny ip any 192.168.20.0 255.255.255.0 log
access-list INSIDE remark Allow outbound services for Internet
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_77309412178
object-group CSM_INLINE_src_rule_77309412178 any
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_77309412202 object
ActiveDirectory.cisco-irn.com any
access-list INSIDE extended permit udp object-group NTP-Servers any eq ntp
access-list INSIDE remark Allow LDAP out LAB test
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_77309412216 object
PAME-DC-1 any log
access-list INSIDE remark Drop and Log all other traffic
access-list INSIDE extended deny ip any any log
access-list OUTSIDE remark Allow SSL VPN
access-list OUTSIDE extended permit tcp any host 192.168.21.1 eq https log
access-list OUTSIDE extended permit udp object-group CSM_INLINE_src_rule_77309412254
object-group NTP-Servers eq ntp
access-list OUTSIDE remark - RIE-2
access-list OUTSIDE extended permit udp object-group CSM_INLINE_src_rule_77309412258
object RSA-enVision eq syslog
access-list OUTSIDE extended permit tcp object-group CSM_INLINE_src_rule_77309412260
object TACACS eq tacacs
access-list OUTSIDE extended permit udp 192.168.21.0 255.255.255.0 object
ActiveDirectory.cisco-irn.com eq domain
access-list OUTSIDE remark Ironport traffic in from DNZ
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_77309412276 host
192.168.23.68 any
access-list OUTSIDE extended permit udp host 192.168.23.68 object RSA-enVision eq syslog
access-list OUTSIDE extended permit udp host 192.168.23.68 object-group NTP-Servers eq ntp

access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_77309412288 host
192.168.23.68 object TACACS
access-list OUTSIDE remark Drop all other traffic
access-list OUTSIDE extended deny ip any any log
access-list all-web webtype permit url any log default
pager lines 24
logging asdm informational
logging host inside 192.168.42.124
mtu outside 1500
mtu inside 1500
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/3
failover link folink GigabitEthernet0/3
failover interface ip folink 192.168.12.31 255.255.255.0 standby 192.168.12.32
icmp unreachable rate-limit 1 burst-size 1
icmp permit any outside
icmp permit any inside
asdm image disk0:/asdm-641.bin
asdm history enable
arp timeout 14400
access-group OUTSIDE in interface outside
access-group INSIDE in interface inside
route outside 0.0.0.0 0.0.0.0 192.168.21.10 1
route inside 10.10.0.0 255.255.0.0 192.168.11.1 1
route outside 10.10.0.0 255.255.255.0 192.168.21.10 1
route inside 192.168.0.0 255.255.0.0 192.168.11.10 1
route outside 192.168.20.0 255.255.255.0 192.168.21.10 1
route outside 192.168.22.0 255.255.255.0 192.168.21.10 1
route outside 192.168.23.0 255.255.255.0 192.168.21.10 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
 network-acl all
 webvpn
  appl-acl all-web
  url-list value page1
  file-browsing enable
  file-entry enable
  http-proxy enable
  url-entry enable
  svc ask enable default webvpn
aaa-server partnerauth protocol radius
aaa-server partnerauth (inside) host 192.168.42.137
 timeout 5
 key *****
 radius-common-pw *****
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (inside) host 192.168.42.131
 key *****
aaa authentication ssh console RETAIL LOCAL
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa accounting ssh console RETAIL
aaa accounting enable console RETAIL
aaa accounting command privilege 15 RETAIL
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
http server enable
http server idle-timeout 15
http server session-timeout 60
http 10.19.151.99 255.255.255.255 inside
http 192.168.41.101 255.255.255.255 inside
http 192.168.41.102 255.255.255.255 inside
http 192.168.42.122 255.255.255.255 inside
http 192.168.42.124 255.255.255.255 inside
http 192.168.42.133 255.255.255.255 inside
http 192.168.42.138 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no snmp-server enable
telnet timeout 5
ssh 10.19.151.99 255.255.255.255 inside
ssh 192.168.41.101 255.255.255.255 inside
ssh 192.168.41.102 255.255.255.255 inside
ssh 192.168.42.122 255.255.255.255 inside
ssh 192.168.42.124 255.255.255.255 inside
ssh 192.168.42.133 255.255.255.255 inside
ssh 192.168.42.138 255.255.255.255 inside
ssh timeout 15
ssh version 2
console timeout 15
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 192.168.62.162 source inside
ntp server 192.168.62.161 source inside prefer
webvpn
 enable outside
 internal-password enable
 smart-tunnel list AllExternalApplications All-Applications * platform windows
group-policy DfltGrpPolicy attributes
 webvpn
  url-list value page1
  smart-tunnel enable AllExternalApplications
group-policy Retail-PCI internal
group-policy Retail-PCI attributes
 vpn-tunnel-protocol ssl-clientless
username csmadmin password  <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
tunnel-group DefaultRAGroup general-attributes
 authentication-server-group partnerauth
tunnel-group DefaultWEBVPNGroup general-attributes
 authentication-server-group partnerauth
tunnel-group Retail-Lab type remote-access
tunnel-group Retail-Lab general-attributes
 authentication-server-group partnerauth LOCAL
 default-group-policy Retail-PCI
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
password encryption aes
Cryptochecksum:7523e3d4b6eac19b34c670de405c3e45
: end
```

ASA-WAN-1

```
: Saved
: Written by retail at 18:21:22.920 PDT Fri Apr 29 2011
!
ASA Version 8.4(1)
!
firewall transparent
hostname ASA-WAN-1
domain-name cisco-irn.com
enable password <removed> encrypted
passwd <removed> encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 bridge-group 1
 security-level 0
!
interface GigabitEthernet0/1
 nameif inside
 bridge-group 1
 security-level 100
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
!
interface GigabitEthernet0/3
 description LAN/STATE Failover Interface
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 management-only
!
interface BVI1
 ip address 192.168.11.20 255.255.255.0 standby 192.168.11.21
!
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
 domain-name cisco-irn.com
object network AdminStation
 host 192.168.41.101
object network AdminStation2
 host 192.168.41.102
object network AdminStation4-bart
 host 10.19.151.99
object network EMC-NCM
 host 192.168.42.122
 description EMC Network Configuration Manager
object network CSManager
 host 192.168.42.133
 description Cisco Security Manager
object network AdminStation3
 host 192.168.42.138
object network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
object network Stores-ALL
 subnet 10.10.0.0 255.255.0.0
 description all store networks
object network vSphere-1
 host 192.168.41.102
 description vSphere server for Lab
object network WCSManager
 host 192.168.43.135
 description Wireless Manager
object network PAME-DC-1
 host 192.168.44.111
object network MSP-DC-1
 host 192.168.44.121
 description Data Center VSOM
object network DC-ALL
 subnet 192.168.0.0 255.255.0.0
 description All of the Data Center
object network RSA-enVision
 host 192.168.42.124
 description RSA EnVision Syslog collector and SIM
object network TACACS
 host 192.168.42.131
 description Csico Secure ACS server for TACACS and Radius
object network RSA-AM
 host 192.168.42.137
 description RSA Authentication Manager for SecureID
object network NAC-2
 host 192.168.42.112
object network NAC-1
 host 192.168.42.111
 description ISE server for NAC
object network MS-Update
 host 192.168.42.150
 description Windows Update Server
object network MSExchange
 host 192.168.42.140
 description Mail Server
object network DC-POS
```

```
 subnet 192.168.52.0 255.255.255.0
 description POS in the Data Center
object service RPC
 service tcp destination eq 135
object service LDAP-GC
 service tcp destination eq 3268
object service LDAP-GC-SSL
 service tcp destination eq 3269
object service Kerberos-TCP
 service tcp destination eq 88
object service Microsoft-DS-SMB
 service tcp destination eq 445
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
object service LDAP-UDP
 service udp destination eq 389
object service RPC-HighPorts
 service tcp destination range 1024 65535
object service IP-Protocol-97
 service 97
 description IP protocol 97
object service TCP1080
 service tcp destination eq 1080
object service TCP8080
 service tcp destination eq 8080
object service RDP
 service tcp destination eq 3389
 description Windows Remote Desktop
object-group network CSM_INLINE_src_rule_73014456577
 description Generated by CS-Manager from src of FirewallRule# 1 (ASA-WAN_1/mandatory)
 network-object object AdminStation
 network-object object AdminStation2
 network-object object AdminStation4-bart
object-group network STORE-POS
 network-object 10.10.0.0 255.255.0.0
object-group network Admin-Systems
 network-object object EMC-NCM
 network-object object AdminStation
 network-object object AdminStation2
 network-object object CSManager
 network-object object AdminStation3
 network-object object AdminStation4-bart
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for stores
 network-object 192.168.43.21 255.255.255.255
 network-object 192.168.43.22 255.255.255.255
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 network-object 192.168.43.31 255.255.255.255
 network-object 192.168.43.32 255.255.255.255
object-group network CSM_INLINE_src_rule_73014456585
 description Generated by CS-Manager from src of FirewallRule# 5 (ASA-WAN_1/mandatory)
 network-object object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
object-group network CSM_INLINE_src_rule_73014456587
 description Generated by CS-Manager from src of FirewallRule# 6 (ASA-WAN_1/mandatory)
 network-object object PAME-DC-1
 network-object object MSP-DC-1
object-group network DC-WAAS
 description WAE Appliances in Data Center
 network-object 192.168.48.10 255.255.255.255
 network-object 192.168.49.10 255.255.255.255
 network-object 192.168.47.11 255.255.255.255
 network-object 192.168.47.12 255.255.255.255
```

```
object-group network NTP-Servers
 description NTP Servers
 network-object 192.168.62.161 255.255.255.255
 network-object 162.168.62.162 255.255.255.255
object-group network CSM_INLINE_dst_rule_73014456607
 description Generated by CS-Manager from dst of FirewallRule# 16 (ASA-WAN_1/mandatory)
 network-object object TACACS
 network-object object RSA-AM
 network-object object NAC-2
 network-object object NAC-1
object-group network CSM_INLINE_dst_rule_73014456609
 description Generated by CS-Manager from dst of FirewallRule# 17 (ASA-WAN_1/mandatory)
 network-object object NAC-2
 network-object object NAC-1
object-group network CSM_INLINE_dst_rule_73014456613
 description Generated by CS-Manager from dst of FirewallRule# 19 (ASA-WAN_1/mandatory)
 network-object object PAME-DC-1
 network-object object MSP-DC-1
object-group network CSM_INLINE_dst_rule_73014456615
 description Generated by CS-Manager from dst of FirewallRule# 20 (ASA-WAN_1/mandatory)
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 network-object 192.168.52.96 255.255.255.224
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 network-object 192.168.52.144 255.255.255.240
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 network-object 192.168.52.128 255.255.255.240
object-group network CSM_INLINE_dst_rule_73014456627
 description Generated by CS-Manager from dst of FirewallRule# 26 (ASA-WAN_1/mandatory)
 group-object DC-POS-Tomax
 network-object object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
object-group service HTTPS-8443
 service-object tcp destination eq 8443
object-group service CSM_INLINE_svc_rule_73014456579
 description Generated by CS-Manager from service of FirewallRule# 2 (ASA-WAN_1/mandatory)
 service-object tcp destination eq ssh
 service-object tcp destination eq https
 group-object HTTPS-8443
object-group service DNS-Resolving
 description Domain Name Server
 service-object tcp destination eq domain
 service-object udp destination eq domain
object-group service CSM_INLINE_svc_rule_73014456581
 description Generated by CS-Manager from service of FirewallRule# 3 (ASA-WAN_1/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq ntp
 service-object udp destination eq netbios-dgm
 service-object object RPC
 service-object object LDAP-GC
 service-object object LDAP-GC-SSL
 service-object object Kerberos-TCP
 service-object object Microsoft-DS-SMB
 service-object object LDAP-UDP
 service-object object RPC-HighPorts
 group-object DNS-Resolving
object-group service vCenter-to-ESX4
```

```
 description Communication from vCetner to ESX hosts
 service-object tcp destination eq 5989
 service-object tcp destination eq 8000
 service-object tcp destination eq 902
 service-object tcp destination eq 903
object-group service CSM_INLINE_svc_rule_73014456583
 description Generated by CS-Manager from service of FirewallRule# 4 (ASA-WAN_1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 group-object vCenter-to-ESX4
object-group service TFTP
 description Trivial File Transfer
 service-object tcp destination eq 69
 service-object udp destination eq tftp
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 service-object udp destination eq 12222
 service-object udp destination eq 12223
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 service-object udp destination eq 5246
 service-object udp destination eq 5247
object-group service CSM_INLINE_svc_rule_73014456585
 description Generated by CS-Manager from service of FirewallRule# 5 (ASA-WAN_1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq www
 service-object udp destination eq isakmp
 service-object tcp destination eq telnet
 service-object tcp destination eq ssh
 service-object object IP-Protocol-97
 group-object TFTP
 group-object LWAPP
 group-object CAPWAP
object-group service CSM_INLINE_svc_rule_73014456589
 description Generated by CS-Manager from service of FirewallRule# 7 (ASA-WAN_1/mandatory)
 service-object icmp echo
 service-object icmp echo-reply
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object tcp destination eq ftp
 service-object object TCP1080
 service-object object TCP8080
 service-object object RDP
 group-object HTTPS-8443
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 service-object tcp destination eq 4050
object-group service Netbios
 description Netbios Servers
 service-object udp destination eq netbios-dgm
 service-object udp destination eq netbios-ns
 service-object tcp destination eq netbios-ssn
object-group service CSM_INLINE_svc_rule_73014456591
 description Generated by CS-Manager from service of FirewallRule# 8 (ASA-WAN_1/mandatory)
 service-object object Microsoft-DS-SMB
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Netbios
object-group service CSM_INLINE_svc_rule_73014456593
 description Generated by CS-Manager from service of FirewallRule# 9 (ASA-WAN_1/mandatory)
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group service CSM_INLINE_svc_rule_73014456599
```

```
 description Generated by CS-Manager from service of FirewallRule# 12
(ASA-WAN_1/mandatory)
 service-object udp destination eq snmptrap
 service-object udp destination eq snmp
 service-object udp destination eq syslog
object-group service CSM_INLINE_svc_rule_73014456601
 description Generated by CS-Manager from service of FirewallRule# 13
(ASA-WAN_1/mandatory)
 service-object udp destination eq domain
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
object-group service CSM_INLINE_svc_rule_73014456607
 description Generated by CS-Manager from service of FirewallRule# 16
(ASA-WAN_1/mandatory)
 service-object udp destination eq 1812
 service-object udp destination eq 1813
object-group service CSM_INLINE_svc_rule_73014456609
 description Generated by CS-Manager from service of FirewallRule# 17
(ASA-WAN_1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq www
 group-object HTTPS-8443
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 service-object udp destination eq 427
 service-object tcp destination eq 427
object-group service CSM_INLINE_svc_rule_73014456611
 description Generated by CS-Manager from service of FirewallRule# 18
(ASA-WAN_1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq www
 service-object tcp destination eq ssh
 group-object vCenter-to-ESX4
 group-object ESX-SLP
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 service-object udp destination eq 16666
 service-object udp destination eq 16667
object-group service CSM_INLINE_svc_rule_73014456615
 description Generated by CS-Manager from service of FirewallRule# 20
(ASA-WAN_1/mandatory)
 service-object tcp destination eq https
 service-object udp destination eq isakmp
 service-object object IP-Protocol-97
 group-object Cisco-Mobility
 group-object LWAPP
 group-object CAPWAP
object-group service CSM_INLINE_svc_rule_73014456617
 description Generated by CS-Manager from service of FirewallRule# 21
(ASA-WAN_1/mandatory)
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group service CSM_INLINE_svc_rule_73014456619
 description Generated by CS-Manager from service of FirewallRule# 22
(ASA-WAN_1/mandatory)
 service-object object Microsoft-DS-SMB
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Netbios
object-group service CSM_INLINE_svc_rule_73014456621
 description Generated by CS-Manager from service of FirewallRule# 23
(ASA-WAN_1/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq ntp
 service-object udp destination eq netbios-dgm
 service-object object RPC
 service-object object LDAP-GC
 service-object object LDAP-GC-SSL
 service-object object Kerberos-TCP
 service-object object Microsoft-DS-SMB
 service-object object LDAP-UDP
 service-object object RPC-HighPorts
 group-object DNS-Resolving
object-group service CSM_INLINE_svc_rule_73014456623
 description Generated by CS-Manager from service of FirewallRule# 24
(ASA-WAN_1/mandatory)
 service-object tcp destination eq www
 service-object tcp destination eq https
object-group service CSM_INLINE_svc_rule_73014456625
 description Generated by CS-Manager from service of FirewallRule# 25
(ASA-WAN_1/mandatory)
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq smtp
 service-object tcp destination eq pop3
 service-object tcp destination eq imap4
object-group network DM_INLINE_NETWORK_1
 network-object 10.10.0.0 255.255.0.0
 network-object object Stores-ALL
object-group service DM_INLINE_SERVICE_1
 service-object tcp destination eq ftp
 service-object tcp destination eq ssh
 service-object udp destination eq tftp
access-list INSIDE extended permit ip object-group CSM_INLINE_src_rule_73014456577
object-group STORE-POS
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_73014456579
object-group Admin-Systems object-group STORE-POS
access-list INSIDE remark Allow Active Directory Domain
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_73014456581 object
ActiveDirectory.cisco-irn.com object Stores-ALL
access-list INSIDE remark VMWare - ESX systems
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_73014456583 object
vSphere-1 object Stores-ALL
access-list INSIDE remark Wireless Management to Stores
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_73014456585
object-group CSM_INLINE_src_rule_73014456585 object Stores-ALL
access-list INSIDE remark Physical security systems
access-list INSIDE extended permit tcp object-group CSM_INLINE_src_rule_73014456587 object
Stores-ALL eq https
access-list INSIDE remark Allow Management of store systems
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_73014456589 object
DC-ALL object Stores-ALL
access-list INSIDE remark WAAS systems
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_73014456591
object-group DC-WAAS object Stores-ALL
access-list INSIDE remark Voice calls
access-list INSIDE extended permit object-group CSM_INLINE_svc_rule_73014456593 object
DC-ALL object Stores-ALL
access-list INSIDE remark Drop and Log all other traffic
access-list INSIDE extended deny ip any any log
access-list OUTSIDE extended permit tcp object Stores-ALL object EMC-NCM eq ssh
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014456599 object
Stores-ALL object RSA-enVision
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014456601 object
Stores-ALL object ActiveDirectory.cisco-irn.com
access-list OUTSIDE extended permit tcp object Stores-ALL object TACACS eq tacacs
```

```
access-list OUTSIDE extended permit udp object Stores-ALL object-group NTP-Servers eq ntp
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014456607 object
Stores-ALL object-group CSM_INLINE_dst_rule_73014456607
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014456609 object
Stores-ALL object-group CSM_INLINE_dst_rule_73014456609
access-list OUTSIDE remark VMWare ESX to Data Center
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014456611 object
Stores-ALL object vSphere-1
access-list OUTSIDE remark Physical security systems
access-list OUTSIDE extended permit tcp object Stores-ALL object-group
CSM_INLINE_dst_rule_73014456613 eq https
access-list OUTSIDE remark Wireless control systems
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014456615 object
Stores-ALL object-group CSM_INLINE_dst_rule_73014456615
access-list OUTSIDE remark Voice calls
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014456617 object
Stores-ALL object DC-ALL
access-list OUTSIDE remark WAAS systems
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014456619 object
Stores-ALL object-group DC-WAAS
access-list OUTSIDE remark Allow Active Directory Domain
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014456621 object
Stores-ALL object ActiveDirectory.cisco-irn.com
access-list OUTSIDE remark Allow Windows Updates
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014456623 object
Stores-ALL object MS-Update
access-list OUTSIDE remark Allow Mail
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014456625 object
Stores-ALL object MSExchange
access-list OUTSIDE remark Allow Applications
access-list OUTSIDE extended permit tcp object Stores-ALL object-group
CSM_INLINE_dst_rule_73014456627 eq https
access-list OUTSIDE extended permit object-group DM_INLINE_SERVICE_1 object-group
DM_INLINE_NETWORK_1 object AdminStation2 log disable
access-list OUTSIDE remark Drop all other traffic
access-list OUTSIDE extended deny ip any any log
pager lines 24
logging host inside 192.168.42.124
mtu outside 1500
mtu inside 1500
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/3
failover link folink GigabitEthernet0/3
failover interface ip folink 192.168.12.20 255.255.255.0 standby 192.168.12.21
icmp unreachable rate-limit 1 burst-size 1
icmp permit any outside
icmp permit any inside
asdm image disk0:/asdm-641.bin
asdm history enable
arp timeout 14400
access-group OUTSIDE in interface outside
access-group INSIDE in interface inside
route inside 0.0.0.0 0.0.0.0 192.168.11.60 1
route outside 10.10.0.0 255.255.0.0 192.168.11.1 1
route inside 10.10.0.0 255.255.255.0 192.168.11.60 1
route outside 10.10.1.0 255.255.255.0 192.168.11.2 1
route outside 10.10.2.0 255.255.255.0 192.168.11.3 1
route inside 10.10.3.0 255.255.255.0 192.168.11.60 1
route inside 10.10.4.0 255.255.255.0 192.168.11.60 1
route outside 10.10.254.0 255.255.255.0 192.168.11.3 1
route outside 10.10.255.0 255.255.255.0 192.168.11.2 1
route inside 192.168.0.0 255.255.0.0 192.168.11.10 1
route outside 192.168.1.111 255.255.255.255 192.168.11.2 1
route outside 192.168.1.112 255.255.255.255 192.168.11.3 1
route inside 192.168.20.0 255.255.252.0 192.168.11.60 1
route inside 192.168.24.0 255.255.255.0 192.168.11.60 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (inside) host 192.168.42.131
 key *****
aaa authentication ssh console RETAIL LOCAL
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa accounting ssh console RETAIL
aaa accounting enable console RETAIL
aaa accounting command privilege 15 RETAIL
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
http server enable
http server idle-timeout 15
http server session-timeout 60
http 192.168.41.102 255.255.255.255 inside
http 10.19.151.99 255.255.255.255 inside
http 192.168.41.101 255.255.255.255 inside
http 192.168.42.122 255.255.255.255 inside
http 192.168.42.124 255.255.255.255 inside
http 192.168.42.133 255.255.255.255 inside
http 192.168.42.138 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no snmp-server enable
telnet timeout 1
ssh scopy enable
ssh 10.19.151.99 255.255.255.255 inside
ssh 192.168.41.101 255.255.255.255 inside
ssh 192.168.41.102 255.255.255.255 inside
ssh 192.168.42.122 255.255.255.255 inside
ssh 192.168.42.124 255.255.255.255 inside
ssh 192.168.42.133 255.255.255.255 inside
ssh 192.168.42.138 255.255.255.255 inside
ssh timeout 15
ssh version 2
console timeout 15
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 192.168.62.162 source inside
ntp server 192.168.62.161 source inside prefer
username csmadmin password <removed> encrypted privilege 15
username retail password <removed>  encrypted privilege 15
username bmcgloth password <removed>  encrypted privilege 15
!
class-map inspection_default
 match default-inspection-traffic
class-map global-class-PCI
 match any
!
!
policy-map type inspect dns preset_dns_map
```

```
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 description IPS inspection policy for Cisco PCI LAB
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
 class global-class-PCI
  ips promiscuous fail-open
!
service-policy global_policy global
prompt hostname context
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
password encryption aes
Cryptochecksum:6711019c0f0a6b2f849474306a18ba82
: end
```

ASA-WAN-1_IDS

```
! ------------------------------
! Current configuration last modified Thu Apr 28 23:24:09 2011
! ------------------------------
! Version 7.0(4)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S500.0   2010-07-09
! ------------------------------
service interface
exit
! ------------------------------
service authentication
attemptLimit 6
password-strength
size 7-64
digits-min 1
```

```
lowercase-min 1
other-min 1
number-old-passwords 4
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 192.168.11.23/24,192.168.11.10
host-name ASA-WAN-1_IPS
telnet-option disabled
access-list 10.19.151.99/32
access-list 192.168.41.101/32
access-list 192.168.41.102/32
access-list 192.168.42.122/32
access-list 192.168.42.124/32
access-list 192.168.42.133/32
access-list 192.168.42.138/32
dns-primary-server enabled
address 192.168.42.130
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.169
port 80
exit
exit
time-zone-settings
offset -8
standard-time-zone-name PST
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 192.168.62.161
exit
summertime-option recurring
summertime-zone-name PDT
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
trap-destinations 192.168.42.124
trap-community-name <removed>
exit
enable-notifications true
trap-community-name <removed>
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
```

```
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
aaa radius
primary-server
server-address 192.168.42.131
shared-secret <removed>
exit
nas-id DMZ-IDS1
local-fallback enabled
console-authentication radius-and-local
default-user-role administrator
exit
exit
! ------------------------------
service analysis-engine
exit
```

ASA-WAN-2_IDS

```
! ------------------------------
! Current configuration last modified Thu Apr 28 23:26:43 2011
! ------------------------------
! Version 7.0(4)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S500.0   2010-07-09
! ------------------------------
service interface
exit
! ------------------------------
service authentication
attemptLimit 6
password-strength
size 7-64
digits-min 1
lowercase-min 1
other-min 1
number-old-passwords 4
exit
exit
! ------------------------------
service event-action-rules rules0
exit
```

```
! ------------------------------
service host
network-settings
host-ip 192.168.11.24/24,192.168.11.10
host-name ASA-WAN-2_IPS
telnet-option disabled
access-list 10.19.151.99/32
access-list 192.168.41.101/32
access-list 192.168.41.102/32
access-list 192.168.42.122/32
access-list 192.168.42.124/32
access-list 192.168.42.133/32
access-list 192.168.42.138/32
dns-primary-server enabled
address 192.168.42.130
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.169
port 80
exit
exit
time-zone-settings
offset -8
standard-time-zone-name PST
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 192.168.62.161
exit
summertime-option recurring
summertime-zone-name PDT
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
trap-destinations 192.168.42.124
trap-community-name <removed>
exit
enable-notifications true
trap-community-name <removed>
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
```

```
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
aaa radius
primary-server
server-address 192.168.42.131
shared-secret <removed>
exit
nas-id DMZ-IDS1
local-fallback enabled
console-authentication radius-and-local
default-user-role administrator
exit
exit
! ------------------------------
service analysis-engine
exit
```

DMZ-ACE-1

```
logging enable
logging timestamp
logging trap 6
logging buffered 6
logging device-id context-name
logging host 192.168.42.124 udp/514
logging rate-limit 1 120 message 302027


login timeout 15
hostname ACE1
boot system image:c6ace-t1k9-mz.3.0.0_A1_4a.bin

resource-class Gold
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource conc-connections minimum 10.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited

tacacs-server host 192.168.42.131 key 7 “<removed>”
aaa group server tacacs+ RETAIL
  server 192.168.42.131


clock timezone standard PST
clock summer-time standard PDT
aaa authentication login default group RETAIL local
aaa authentication login console group RETAIL local
aaa accounting default group RETAIL local



class-map type management match-any remote-mgmt
```

```
  9 match protocol ssh source-address 192.168.41.102 255.255.255.255
  10 match protocol ssh source-address 192.168.42.131 255.255.255.255
  30 match protocol icmp any
  31 match protocol ssh source-address 10.19.151.99 255.255.255.255
  32 match protocol ssh source-address 192.168.41.101 255.255.255.255
  33 match protocol ssh source-address 192.168.42.111 255.255.255.255
  34 match protocol ssh source-address 192.168.42.122 255.255.255.255
  35 match protocol ssh source-address 192.168.42.124 255.255.255.255
  36 match protocol ssh source-address 192.168.42.133 255.255.255.255
  37 match protocol ssh source-address 192.168.42.138 255.255.255.255

policy-map type management first-match remote-access
  class remote-mgmt
    permit

interface vlan 21
  ip address 192.168.21.95 255.255.255.0
  service-policy input remote-access
  no shutdown

ft interface vlan 85
  ip address 192.168.20.9 255.255.255.252
  peer ip address 192.168.20.10 255.255.255.252
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 85
ft group 11
  peer 1
  priority 110
  peer priority 105
  associate-context Admin
  inservice

domain cisco-irn.com

ip route 0.0.0.0 0.0.0.0 192.168.21.1

context PCI
  allocate-interface vlan 82-83
  allocate-interface vlan 95



ft group 10
  peer 1
  priority 110
  peer priority 105
  associate-context PCI
  inservice
username admin password 5 <removed>   role Admin domain default-domain
username www password 5 <removed>   role Admin domain default-domain
username retail password 5 <removed>   role Admin domain default-domain
username csmadmin password 5 <removed>   role Admin domain default-domain
ssh key rsa 1024 force
```

DMZ-ACE-1_PCI

```
ACE1/PCI# sh run
Generating configuration....

logging enable
logging timestamp
logging buffered 7
logging monitor 7
logging device-id context-name
logging host 192.168.42.124 udp/514
logging rate-limit 1 120 message 302027


login timeout 15

tacacs-server host 192.168.42.131 key 7 “<removed>”
aaa group server tacacs+ RETAIL
  server 192.168.42.131
aaa authentication login default group RETAIL local
aaa authentication login console group RETAIL local
aaa accounting default group RETAIL local

access-list allow2server line 20 extended permit ip any host 192.168.20.3
access-list allow2server line 21 extended permit tcp host 192.168.20.44 host 192
.168.42.130 eq ldap
access-list allow2server line 22 extended deny ip any any
access-list in2out line 10 extended permit ip host 192.168.20.3 any
access-list in2out line 15 extended deny ip any any
access-list out2in line 10 extended permit tcp any host 192.168.20.1 eq www
access-list out2in line 15 extended deny ip any any


probe icmp ICMP
  interval 2
  faildetect 2
  passdetect interval 60
  passdetect count 2

rserver host ECOM
  ip address 192.168.20.44
  inservice

serverfarm host PCI-ECOM
  predictor leastconns
  probe ICMP
  rserver ECOM
    inservice

class-map match-any ECOMVIP
  11 match virtual-address 192.168.20.1 any
class-map type management match-any remote-mgmt
  30 match protocol icmp any
  31 match protocol ssh source-address 10.19.151.99 255.255.255.255
  32 match protocol ssh source-address 192.168.41.101 255.255.255.255
  33 match protocol ssh source-address 192.168.41.102 255.255.255.255
  34 match protocol ssh source-address 192.168.42.111 255.255.255.255
  35 match protocol ssh source-address 192.168.42.122 255.255.255.255
  36 match protocol ssh source-address 192.168.42.124 255.255.255.255
  37 match protocol ssh source-address 192.168.42.131 255.255.255.255
  38 match protocol ssh source-address 192.168.42.133 255.255.255.255
  39 match protocol ssh source-address 192.168.42.138 255.255.255.255
```

```
policy-map type management first-match remote-access
  class remote-mgmt
    permit
policy-map type loadbalance first-match ECOMPOLICY
  class class-default
    serverfarm PCI-ECOM
policy-map multi-match ECOM_MATCH
  class ECOMVIP
    loadbalance vip inservice
    loadbalance policy ECOMPOLICY

service-policy input remote-access

interface vlan 82
  description ACE_outside
  ip address 192.168.20.28 255.255.255.248
  ip verify reverse-path
  alias 192.168.20.30 255.255.255.248
  peer ip address 192.168.20.29 255.255.255.248
  access-group input out2in
  service-policy input ECOM_MATCH
  no shutdown
interface vlan 83
  description ACE_inside
  ip address 192.168.20.4 255.255.255.248
  ip verify reverse-path
  alias 192.168.20.6 255.255.255.248
  peer ip address 192.168.20.5 255.255.255.248
  access-group input in2out
  no shutdown

domain cisco-irn.com

ip route 0.0.0.0 0.0.0.0 192.168.20.25
username csmadmin password 5 <removed>   role Admin doma
in default-domain
username retail password 5 <removed>   role Admin domain
 default-domain
username bmcgloth password 5 <removed>   role Admin doma
in default-domain
```

DMZ-ACE-2_Admin

```
ACE2/Admin# sh run
Generating configuration....

logging enable
logging timestamp
logging trap 6
logging buffered 6
logging device-id context-name
logging host 192.168.42.124 udp/514
logging rate-limit 1 120 message 302027


login timeout 15
hostname ACE2
boot system image:c6ace-t1k9-mz.3.0.0_A1_4a.bin

resource-class Gold
```

```
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource conc-connections minimum 10.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited


tacacs-server host 192.168.42.131 key 7 "<removed>"
aaa group server tacacs+ RETAIL
  server 192.168.42.131

clock timezone standard PST
clock summer-time standard PDT
aaa authentication login default group RETAIL local
aaa authentication login console group RETAIL local
aaa accounting default group RETAIL local



class-map type management match-any remote-mgmt
  9 match protocol ssh source-address 192.168.41.102 255.255.255.255
  10 match protocol ssh source-address 192.168.42.131 255.255.255.255
  30 match protocol icmp any
  31 match protocol ssh source-address 10.19.151.99 255.255.255.255
  32 match protocol ssh source-address 192.168.41.101 255.255.255.255
  33 match protocol ssh source-address 192.168.42.111 255.255.255.255
  34 match protocol ssh source-address 192.168.42.122 255.255.255.255
  35 match protocol ssh source-address 192.168.42.124 255.255.255.255
  36 match protocol ssh source-address 192.168.42.133 255.255.255.255
  37 match protocol ssh source-address 192.168.42.138 255.255.255.255

policy-map type management first-match remote-access
  class remote-mgmt
    permit

interface vlan 21
  peer ip address 192.168.21.95 255.255.255.0
  service-policy input remote-access
  no shutdown

ft interface vlan 85
  ip address 192.168.20.10 255.255.255.252
  peer ip address 192.168.20.9 255.255.255.252
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 85
ft group 11
  peer 1
  priority 105
  peer priority 110
  associate-context Admin
  inservice

domain cisco-irn.com

ip route 0.0.0.0 0.0.0.0 192.168.21.1

context PCI
  allocate-interface vlan 82-83
  allocate-interface vlan 95
```

```
ft group 10
  peer 1
  priority 105
  peer priority 110
  associate-context PCI
  inservice
username admin password 5 <removed>   role Admin domain
default-domain
username www password 5 <removed>   role Admin domain de
fault-domain
username retail password 5 <removed>   role Admin domain
 default-domain
username csmadmin password 5 <removed>   role Admin doma
in default-domain
ssh key rsa 1024 force

ACE2/Admin#
```

DMZ-ACE-2_PCI

```
ACE2/PCI# sh run
Generating configuration....

logging enable
logging timestamp
logging buffered 7
logging monitor 7
logging device-id context-name
logging host 192.168.42.124 udp/514
logging rate-limit 1 120 message 302027


login timeout 15

tacacs-server host 192.168.42.131 key 7 "<removed>"
aaa group server tacacs+ RETAIL
  server 192.168.42.131
aaa authentication login default group RETAIL local
aaa authentication login console group RETAIL local
aaa accounting default group RETAIL local

access-list allow2server line 20 extended permit ip any host 192.168.20.3
access-list allow2server line 21 extended permit tcp host 192.168.20.44 host 192
.168.42.130 eq ldap
access-list allow2server line 22 extended deny ip any any
access-list in2out line 10 extended permit ip host 192.168.20.3 any
access-list in2out line 15 extended deny ip any any
access-list out2in line 10 extended permit tcp any host 192.168.20.1 eq www
access-list out2in line 15 extended deny ip any any


probe icmp ICMP
  interval 2
  faildetect 2
  passdetect interval 60
  passdetect count 2

rserver host ECOM
  ip address 192.168.20.44
  inservice
```

```
serverfarm host PCI-ECOM
  predictor leastconns
  probe ICMP
  rserver ECOM
    inservice

class-map match-any ECOMVIP
  11 match virtual-address 192.168.20.1 any
class-map type management match-any remote-mgmt
  30 match protocol icmp any
  31 match protocol ssh source-address 10.19.151.99 255.255.255.255
  32 match protocol ssh source-address 192.168.41.101 255.255.255.255
  33 match protocol ssh source-address 192.168.41.102 255.255.255.255
  34 match protocol ssh source-address 192.168.42.111 255.255.255.255
  35 match protocol ssh source-address 192.168.42.122 255.255.255.255
  36 match protocol ssh source-address 192.168.42.124 255.255.255.255
  37 match protocol ssh source-address 192.168.42.131 255.255.255.255
  38 match protocol ssh source-address 192.168.42.133 255.255.255.255
  39 match protocol ssh source-address 192.168.42.138 255.255.255.255

policy-map type management first-match remote-access
  class remote-mgmt
    permit
policy-map type loadbalance first-match ECOMPOLICY
  class class-default
    serverfarm PCI-ECOM
policy-map multi-match ECOM_MATCH
  class ECOMVIP
    loadbalance vip inservice
    loadbalance policy ECOMPOLICY

service-policy input remote-access

interface vlan 82
  description ACE_outside
  ip address 192.168.20.29 255.255.255.248
  ip verify reverse-path
  alias 192.168.20.30 255.255.255.248
  peer ip address 192.168.20.28 255.255.255.248
  access-group input out2in
  service-policy input ECOM_MATCH
  no shutdown
interface vlan 83
  description ACE_inside
  ip address 192.168.20.5 255.255.255.248
  ip verify reverse-path
  alias 192.168.20.6 255.255.255.248
  peer ip address 192.168.20.4 255.255.255.248
  access-group input in2out
  no shutdown

domain cisco-irn.com

ip route 0.0.0.0 0.0.0.0 192.168.20.25
username csmadmin password 5 <removed>   role Admin doma
in default-domain
username retail password 5 <removed>   role Admin domain
 default-domain
username bmcgloth password 5 <removed>   role Admin doma
in default-domain
```

```
ACE2/PCI#
```

DMZ-IDS-1

```
! ------------------------------
! Current configuration last modified Thu Apr 28 21:34:42 2011
! ------------------------------
! Version 7.0(4)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S500.0   2010-07-09
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/7
subinterface-type inline-vlan-pair
subinterface 1
description INT1 vlans 83 and 84
vlan1 83
vlan2 84
exit
exit
exit
exit
! ------------------------------
service authentication
attemptLimit 6
password-strength
size 7-64
digits-min 1
lowercase-min 1
other-min 1
number-old-passwords 4
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 192.168.21.93/24,192.168.21.1
host-name DMZ-IDS1
telnet-option disabled
access-list 10.19.151.99/32
access-list 192.168.41.101/32
access-list 192.168.41.102/32
access-list 192.168.42.122/32
access-list 192.168.42.124/32
access-list 192.168.42.133/32
access-list 192.168.42.138/32
dns-primary-server enabled
address 192.168.42.130
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.169
port 80
exit
```

```
exit
time-zone-settings
offset -8
standard-time-zone-name PST
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 192.168.62.161
exit
summertime-option recurring
summertime-zone-name PDT
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
trap-destinations 192.168.42.124
trap-community-name <removed>
exit
enable-notifications true
trap-community-name <removed>
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
aaa radius
primary-server
server-address 192.168.42.131
shared-secret <removed>
exit
nas-id DMZ-IDS1
local-fallback enabled
console-authentication radius-and-local
default-user-role administrator
exit
exit
! ------------------------------
```

```
service analysis-engine
exit
```

DMZ-IDSM2

```
! ------------------------------
! Current configuration last modified Thu Apr 28 22:06:38 2011
! ------------------------------
! Version 7.0(4)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S500.0   2010-07-09
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/7
subinterface-type inline-vlan-pair
subinterface 1
description INT1 vlans 83 and 84
vlan1 83
vlan2 84
exit
exit
exit
exit
! ------------------------------
service authentication
attemptLimit 6
password-strength
size 7-64
digits-min 1
lowercase-min 1
other-min 1
number-old-passwords 4
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 192.168.21.94/24,192.168.21.1
host-name DMZ-IDS2
telnet-option disabled
access-list 10.19.151.99/32
access-list 192.168.41.101/32
access-list 192.168.41.102/32
access-list 192.168.42.122/32
access-list 192.168.42.124/32
access-list 192.168.42.133/32
access-list 192.168.42.138/32
dns-primary-server enabled
address 192.168.42.130
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.169
port 80
exit
```

```
exit
time-zone-settings
offset -8
standard-time-zone-name PST
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 192.168.62.161
exit
summertime-option recurring
summertime-zone-name PDT
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
trap-destinations 192.168.42.124
trap-community-name <removed>
exit
enable-notifications true
trap-community-name <removed>
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
aaa radius
primary-server
server-address 192.168.42.131
shared-secret <removed>
exit
nas-id DMZ-IDS1
local-fallback enabled
console-authentication radius-and-local
default-user-role administrator
exit
exit
! ------------------------------
```

```
service analysis-engine
exit
```

FW-A2-MSP-1

```
: Saved
: Written by retail at 18:15:18.945 PDT Fri Apr 29 2011
!
ASA Version 8.4(1)
!
hostname FW-A2-MSP-1
domain-name cisco-irn.com
enable password <removed>  encrypted
passwd <removed>  encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif MSP-WAN
 security-level 0
 ip address 10.10.255.176 255.255.255.0
!
interface Ethernet0/1
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/1.11
 vlan 11
 nameif POS
 security-level 95
 ip address 10.10.176.1 255.255.255.0
!
interface Ethernet0/1.12
 vlan 12
 nameif DATA
 security-level 85
 ip address 10.10.177.1 255.255.255.0
!
interface Ethernet0/1.13
 vlan 13
 nameif VOICE
 security-level 80
 ip address 10.10.178.1 255.255.255.0
!
interface Ethernet0/1.14
 vlan 14
 nameif WIRELESS
 security-level 70
 ip address 10.10.179.1 255.255.255.0
!
interface Ethernet0/1.15
 vlan 15
 nameif WIRELESS-POS
 security-level 90
 ip address 10.10.180.1 255.255.255.0
!
interface Ethernet0/1.16
 vlan 16
 nameif PARTNER
 security-level 65
 ip address 10.10.181.1 255.255.255.0
!
interface Ethernet0/1.17
 vlan 17
 nameif WIRELESS-GUEST
 security-level 10
 ip address 10.10.182.1 255.255.255.0
!
interface Ethernet0/1.18
 vlan 18
 nameif WIRELESS-CONTROL
 security-level 75
 ip address 10.10.183.1 255.255.255.0
!
interface Ethernet0/1.19
 vlan 19
 nameif WAAS
 security-level 100
 ip address 10.10.184.1 255.255.255.0
!
interface Ethernet0/1.1000
 vlan 1000
 nameif MANAGEMENT
 security-level 100
 ip address 10.10.191.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
 domain-name cisco-irn.com
same-security-traffic permit inter-interface
object network AdminStation
 host 192.168.41.101
object network AdminStation2
 host 192.168.41.102
object network AdminStation4-bart
 host 10.19.151.99
object network EMC-NCM
 host 192.168.42.122
 description EMC Network Configuration Manager
object network CSManager
 host 192.168.42.133
 description Cisco Security Manager
object network AdminStation3
 host 192.168.42.138
```

```
object network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
object network DC-POS
 subnet 192.168.52.0 255.255.255.0
 description POS in the Data Center
object network WCSManager
 host 192.168.43.135
 description Wireless Manager
object network PAME-DC-1
 host 192.168.44.111
object network MSP-DC-1
 host 192.168.44.121
 description Data Center VSOM
object network DC-ALL
 subnet 192.168.0.0 255.255.0.0
 description All of the Data Center
object network RSA-enVision
 host 192.168.42.124
 description RSA EnVision Syslog collector and SIM
object network TACACS
 host 192.168.42.131
 description Csico Secure ACS server for TACACS and Radius
object network RSA-AM
 host 192.168.42.137
 description RSA Authentication Manager for SecureID
object network NAC-2
 host 192.168.42.112
object network NAC-1
 host 192.168.42.111
 description ISE server for NAC
object network MS-Update
 host 192.168.42.150
 description Windows Update Server
object network MSExchange
 host 192.168.42.140
 description Mail Server
object service RPC
 service tcp destination eq 135
object service LDAP-GC
 service tcp destination eq 3268
object service LDAP-GC-SSL
 service tcp destination eq 3269
object service Kerberos-TCP
 service tcp destination eq 88
object service Microsoft-DS-SMB
 service tcp destination eq 445
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
object service LDAP-UDP
 service udp destination eq 389
object service RPC-HighPorts
 service tcp destination range 1024 65535
object service ORACLE-OAS
 service tcp destination eq 12601
 description OAS uses one port for HTTP and RMI - 12601.
object service TOMAX-8990
 service tcp destination eq 8990
 description Tomax Application Port
object service IP-Protocol-97
 service 97
 description IP protocol 97
object service TCP1080
 service tcp destination eq 1080
object service TCP8080
 service tcp destination eq 8080
```

```
object service RDP
 service tcp destination eq 3389
 description Windows Remote Desktop
object-group network CSM_INLINE_src_rule_73014461090
 description Generated by CS-Manager from src of FirewallRule# 1 (ASA-Store_V2/mandatory)
 network-object object AdminStation
 network-object object AdminStation2
 network-object object AdminStation4-bart
object-group network Admin-Systems
 network-object object EMC-NCM
 network-object object AdminStation
 network-object object AdminStation2
 network-object object CSManager
 network-object object AdminStation3
 network-object object AdminStation4-bart
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 network-object 192.168.52.96 255.255.255.224
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 network-object 192.168.52.144 255.255.255.240
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 network-object 192.168.52.128 255.255.255.240
object-group network CSM_INLINE_src_rule_73014461184
 description Generated by CS-Manager from src of FirewallRule# 4 (ASA-Store_V2/mandatory)
 group-object DC-POS-Tomax
 network-object object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
object-group network POS-Store-MSP
 network-object 10.10.176.81 255.255.255.255
object-group network CSM_INLINE_dst_rule_73014461438
 description Generated by CS-Manager from dst of FirewallRule# 5 (ASA-Store_V2/mandatory)
 group-object DC-POS-Tomax
 network-object object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
object-group network Store-MSP-POS-net
 network-object 10.10.176.0 255.255.255.0
 network-object 10.10.180.0 255.255.255.0
object-group network CSM_INLINE_dst_rule_73014461436
 description Generated by CS-Manager from dst of FirewallRule# 7 (ASA-Store_V2/mandatory)
 group-object DC-POS-Tomax
 network-object object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for stores
 network-object 192.168.43.21 255.255.255.255
 network-object 192.168.43.22 255.255.255.255
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 network-object 192.168.43.31 255.255.255.255
 network-object 192.168.43.32 255.255.255.255
object-group network CSM_INLINE_src_rule_73014461098
 description Generated by CS-Manager from src of FirewallRule# 8 (ASA-Store_V2/mandatory)
 network-object object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
object-group network CSM_INLINE_src_rule_73014461100
 description Generated by CS-Manager from src of FirewallRule# 9 (ASA-Store_V2/mandatory)
 network-object object PAME-DC-1
 network-object object MSP-DC-1
```

```
object-group network DC-WAAS
 description WAE Appliances in Data Center
 network-object 192.168.48.10 255.255.255.255
 network-object 192.168.49.10 255.255.255.255
 network-object 192.168.47.11 255.255.255.255
 network-object 192.168.47.12 255.255.255.255
object-group network NTP-Servers
 description NTP Servers
 network-object 192.168.62.161 255.255.255.255
 network-object 162.168.62.162 255.255.255.255
object-group network CSM_INLINE_dst_rule_73014461120
 description Generated by CS-Manager from dst of FirewallRule# 17 (ASA-Store_V2/mandatory)
 network-object object TACACS
 network-object object RSA-AM
 network-object object NAC-2
 network-object object NAC-1
object-group network CSM_INLINE_dst_rule_73014461126
 description Generated by CS-Manager from dst of FirewallRule# 18 (ASA-Store_V2/mandatory)
 network-object object PAME-DC-1
 network-object object MSP-DC-1
object-group network CSM_INLINE_dst_rule_73014461128
 description Generated by CS-Manager from dst of FirewallRule# 19 (ASA-Store_V2/mandatory)
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
object-group service HTTPS-8443
 service-object tcp destination eq 8443
object-group service CSM_INLINE_svc_rule_73014461092
 description Generated by CS-Manager from service of FirewallRule# 2
(ASA-Store_V2/mandatory)
 service-object tcp destination eq ssh
 service-object tcp destination eq https
 group-object HTTPS-8443
object-group service DNS-Resolving
 description Domain Name Server
 service-object tcp destination eq domain
 service-object udp destination eq domain
object-group service CSM_INLINE_svc_rule_73014461094
 description Generated by CS-Manager from service of FirewallRule# 3
(ASA-Store_V2/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq ntp
 service-object udp destination eq netbios-dgm
 service-object object RPC
 service-object object LDAP-GC
 service-object object LDAP-GC-SSL
 service-object object Kerberos-TCP
 service-object object Microsoft-DS-SMB
 service-object object LDAP-UDP
 service-object object RPC-HighPorts
 group-object DNS-Resolving
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 service-object tcp destination range 1300 1319
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 service-object tcp destination eq 7001
 service-object tcp destination eq 7002
 service-object tcp destination eq sqlnet
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 service-object tcp destination eq 2809
 service-object tcp destination eq 9443
 service-object tcp destination eq 1414
object-group service CSM_INLINE_svc_rule_73014461184
 description Generated by CS-Manager from service of FirewallRule# 4
(ASA-Store_V2/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object object ORACLE-OAS
 service-object object TOMAX-8990
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object HTTPS-8443
object-group service TFTP
 description Trivial File Transfer
 service-object tcp destination eq 69
 service-object udp destination eq tftp
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 service-object udp destination eq 12222
 service-object udp destination eq 12223
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 service-object udp destination eq 5246
 service-object udp destination eq 5247
object-group service CSM_INLINE_svc_rule_73014461098
 description Generated by CS-Manager from service of FirewallRule# 8
(ASA-Store_V2/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq www
 service-object udp destination eq isakmp
 service-object tcp destination eq telnet
 service-object tcp destination eq ssh
 service-object object IP-Protocol-97
 group-object TFTP
 group-object LWAPP
 group-object CAPWAP
object-group service CSM_INLINE_svc_rule_73014461102
 description Generated by CS-Manager from service of FirewallRule# 10
(ASA-Store_V2/mandatory)
 service-object icmp echo
 service-object icmp echo-reply
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object tcp destination eq ftp
 service-object object TCP1080
 service-object object TCP8080
 service-object object RDP
 group-object HTTPS-8443
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 service-object tcp destination eq 4050
object-group service Netbios
 description Netbios Servers
 service-object udp destination eq netbios-dgm
 service-object udp destination eq netbios-ns
 service-object tcp destination eq netbios-ssn
object-group service CSM_INLINE_svc_rule_73014461104
 description Generated by CS-Manager from service of FirewallRule# 11
(ASA-Store_V2/mandatory)
 service-object object Microsoft-DS-SMB
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Netbios
```

```
object-group service CSM_INLINE_svc_rule_73014461106
 description Generated by CS-Manager from service of FirewallRule# 12
(ASA-Store_V2/mandatory)
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group service CSM_INLINE_svc_rule_73014461112
 description Generated by CS-Manager from service of FirewallRule# 14
(ASA-Store_V2/mandatory)
 service-object udp destination eq snmptrap
 service-object udp destination eq snmp
 service-object udp destination eq syslog
object-group service CSM_INLINE_svc_rule_73014461120
 description Generated by CS-Manager from service of FirewallRule# 17
(ASA-Store_V2/mandatory)
 service-object udp destination eq 1812
 service-object udp destination eq 1813
 service-object tcp destination eq https
 service-object tcp destination eq www
 group-object HTTPS-8443
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 service-object udp destination eq 16666
 service-object udp destination eq 16667
object-group service CSM_INLINE_svc_rule_73014461128
 description Generated by CS-Manager from service of FirewallRule# 19
(ASA-Store_V2/mandatory)
 service-object tcp destination eq https
 service-object udp destination eq isakmp
 service-object object IP-Protocol-97
 group-object Cisco-Mobility
 group-object LWAPP
 group-object CAPWAP
object-group service CSM_INLINE_svc_rule_73014461130
 description Generated by CS-Manager from service of FirewallRule# 20
(ASA-Store_V2/mandatory)
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group service CSM_INLINE_svc_rule_73014461132
 description Generated by CS-Manager from service of FirewallRule# 21
(ASA-Store_V2/mandatory)
 service-object object Microsoft-DS-SMB
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Netbios
object-group service CSM_INLINE_svc_rule_73014461134
 description Generated by CS-Manager from service of FirewallRule# 22
(ASA-Store_V2/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq ntp
 service-object udp destination eq netbios-dgm
 service-object object RPC
 service-object object LDAP-GC
 service-object object LDAP-GC-SSL
 service-object object Kerberos-TCP
 service-object object Microsoft-DS-SMB
 service-object object LDAP-UDP
 service-object object RPC-HighPorts
 group-object DNS-Resolving
object-group service CSM_INLINE_svc_rule_73014461136
 description Generated by CS-Manager from service of FirewallRule# 23
(ASA-Store_V2/mandatory)
 service-object tcp destination eq www
 service-object tcp destination eq https
object-group service CSM_INLINE_svc_rule_73014461138
 description Generated by CS-Manager from service of FirewallRule# 24
(ASA-Store_V2/mandatory)
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq smtp
 service-object tcp destination eq pop3
 service-object tcp destination eq imap4
access-list OUTSIDE remark LAB Testing
access-list OUTSIDE extended permit ip object-group CSM_INLINE_src_rule_73014461090
10.10.176.0 255.255.248.0
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461092
object-group Admin-Systems 10.10.176.0 255.255.248.0
access-list OUTSIDE remark Allow Active Directory Domain
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461094 object
ActiveDirectory.cisco-irn.com 10.10.176.0 255.255.248.0
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461184
object-group CSM_INLINE_src_rule_73014461184 object-group POS-Store-MSP
access-list OUTSIDE extended deny ip any object-group Store-MSP-POS-net
access-list OUTSIDE extended deny ip any object-group CSM_INLINE_dst_rule_73014461436
access-list OUTSIDE remark Wireless Management to Stores
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461098
object-group CSM_INLINE_src_rule_73014461098 10.10.183.0 255.255.255.0
access-list OUTSIDE remark Physical security systems
access-list OUTSIDE extended permit tcp object-group CSM_INLINE_src_rule_73014461100
10.10.191.0 255.255.255.0 eq https
access-list OUTSIDE remark Allow Management of store systems
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461102 object
DC-ALL 10.10.176.0 255.255.248.0
access-list OUTSIDE remark WAAS systems
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461104
object-group DC-WAAS 10.10.184.0 255.255.255.0
access-list OUTSIDE remark Voice calls
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461106 object
DC-ALL 10.10.178.0 255.255.255.0
access-list OUTSIDE extended permit tcp 10.10.176.0 255.255.248.0 object EMC-NCM eq ssh
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461112
10.10.176.0 255.255.248.0 object RSA-enVision
access-list OUTSIDE extended permit tcp 10.10.176.0 255.255.248.0 object TACACS eq tacacs
access-list OUTSIDE extended permit udp 10.10.176.0 255.255.248.0 object-group NTP-Servers
eq ntp
access-list OUTSIDE remark Drop all other traffic
access-list OUTSIDE extended deny ip any any log
access-list CSM_FW_ACL_POS remark Allow Applications
access-list CSM_FW_ACL_POS extended permit tcp object-group POS-Store-MSP object-group
CSM_INLINE_dst_rule_73014461438 eq https
access-list CSM_FW_ACL_POS extended deny ip any object-group Store-MSP-POS-net
access-list CSM_FW_ACL_POS extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
access-list CSM_FW_ACL_POS extended permit udp 10.10.176.0 255.255.248.0 object-group
NTP-Servers eq ntp
access-list CSM_FW_ACL_POS extended permit object-group CSM_INLINE_svc_rule_73014461120
10.10.176.0 255.255.248.0 object-group CSM_INLINE_dst_rule_73014461120
access-list CSM_FW_ACL_POS remark Allow Active Directory Domain
access-list CSM_FW_ACL_POS extended permit object-group CSM_INLINE_svc_rule_73014461134
10.10.176.0 255.255.248.0 object ActiveDirectory.cisco-irn.com
access-list CSM_FW_ACL_POS remark Allow Windows Updates
access-list CSM_FW_ACL_POS extended permit object-group CSM_INLINE_svc_rule_73014461136
10.10.176.0 255.255.248.0 object MS-Update
access-list CSM_FW_ACL_POS remark Allow Mail
access-list CSM_FW_ACL_POS extended permit object-group CSM_INLINE_svc_rule_73014461138
10.10.176.0 255.255.248.0 object MSExchange
access-list CSM_FW_ACL_POS remark Drop all other traffic
```

```
access-list CSM_FW_ACL_POS extended deny ip any any log
access-list CSM_FW_ACL_WIRELESS-POS remark Allow Applications
access-list CSM_FW_ACL_WIRELESS-POS extended permit tcp object-group POS-Store-MSP
object-group CSM_INLINE_dst_rule_73014461438 eq https
access-list CSM_FW_ACL_WIRELESS-POS extended deny ip any object-group Store-MSP-POS-net
access-list CSM_FW_ACL_WIRELESS-POS extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
access-list CSM_FW_ACL_WIRELESS-POS extended permit udp 10.10.176.0 255.255.248.0
object-group NTP-Servers eq ntp
access-list CSM_FW_ACL_WIRELESS-POS remark Allow Active Directory Domain
access-list CSM_FW_ACL_WIRELESS-POS extended permit object-group
CSM_INLINE_svc_rule_73014461134 10.10.176.0 255.255.248.0 object
ActiveDirectory.cisco-irn.com
access-list CSM_FW_ACL_WIRELESS-POS remark Allow Windows Updates
access-list CSM_FW_ACL_WIRELESS-POS extended permit object-group
CSM_INLINE_svc_rule_73014461136 10.10.176.0 255.255.248.0 object MS-Update
access-list CSM_FW_ACL_WIRELESS-POS remark Allow Mail
access-list CSM_FW_ACL_WIRELESS-POS extended permit object-group
CSM_INLINE_svc_rule_73014461138 10.10.176.0 255.255.248.0 object MSExchange
access-list CSM_FW_ACL_WIRELESS-POS remark Drop all other traffic
access-list CSM_FW_ACL_WIRELESS-POS extended deny ip any any log
access-list CSM_FW_ACL_DATA extended deny ip any object-group Store-MSP-POS-net
access-list CSM_FW_ACL_DATA extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
access-list CSM_FW_ACL_DATA extended permit udp 10.10.176.0 255.255.248.0 object-group
NTP-Servers eq ntp
access-list CSM_FW_ACL_DATA extended permit object-group CSM_INLINE_svc_rule_73014461120
10.10.176.0 255.255.248.0 object-group CSM_INLINE_dst_rule_73014461120
access-list CSM_FW_ACL_DATA remark Allow Active Directory Domain
access-list CSM_FW_ACL_DATA extended permit object-group CSM_INLINE_svc_rule_73014461134
10.10.176.0 255.255.248.0 object ActiveDirectory.cisco-irn.com
access-list CSM_FW_ACL_DATA remark Allow Windows Updates
access-list CSM_FW_ACL_DATA extended permit object-group CSM_INLINE_svc_rule_73014461136
10.10.176.0 255.255.248.0 object MS-Update
access-list CSM_FW_ACL_DATA remark Allow Mail
access-list CSM_FW_ACL_DATA extended permit object-group CSM_INLINE_svc_rule_73014461138
10.10.176.0 255.255.248.0 object MSExchange
access-list CSM_FW_ACL_DATA remark Drop all other traffic
access-list CSM_FW_ACL_DATA extended deny ip any any log
access-list CSM_FW_ACL_MANAGEMENT extended deny ip any object-group Store-MSP-POS-net
access-list CSM_FW_ACL_MANAGEMENT extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
access-list CSM_FW_ACL_MANAGEMENT extended permit tcp 10.10.176.0 255.255.248.0 object
EMC-NCM eq ssh
access-list CSM_FW_ACL_MANAGEMENT extended permit object-group
CSM_INLINE_svc_rule_73014461112 10.10.176.0 255.255.248.0 object RSA-enVision
access-list CSM_FW_ACL_MANAGEMENT extended permit tcp 10.10.176.0 255.255.248.0 object
TACACS eq tacacs
access-list CSM_FW_ACL_MANAGEMENT extended permit udp 10.10.176.0 255.255.248.0
object-group NTP-Servers eq ntp
access-list CSM_FW_ACL_MANAGEMENT extended permit object-group
CSM_INLINE_svc_rule_73014461120 10.10.176.0 255.255.248.0 object-group
CSM_INLINE_dst_rule_73014461120
access-list CSM_FW_ACL_MANAGEMENT remark Physical security systems
access-list CSM_FW_ACL_MANAGEMENT extended permit tcp 10.10.191.0 255.255.255.0
object-group CSM_INLINE_dst_rule_73014461126 eq https
access-list CSM_FW_ACL_MANAGEMENT remark Allow Mail
access-list CSM_FW_ACL_MANAGEMENT extended permit object-group
CSM_INLINE_svc_rule_73014461138 10.10.176.0 255.255.248.0 object MSExchange
access-list CSM_FW_ACL_MANAGEMENT remark Drop all other traffic
access-list CSM_FW_ACL_MANAGEMENT extended deny ip any any log
access-list CSM_FW_ACL_PARTNER extended deny ip any object-group Store-MSP-POS-net
access-list CSM_FW_ACL_PARTNER extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
```

```
access-list CSM_FW_ACL_PARTNER extended permit udp 10.10.176.0 255.255.248.0 object-group
NTP-Servers eq ntp
access-list CSM_FW_ACL_PARTNER extended permit object-group
CSM_INLINE_svc_rule_73014461120 10.10.176.0 255.255.248.0 object-group
CSM_INLINE_dst_rule_73014461120
access-list CSM_FW_ACL_PARTNER remark Allow Mail
access-list CSM_FW_ACL_PARTNER extended permit object-group
CSM_INLINE_svc_rule_73014461138 10.10.176.0 255.255.248.0 object MSExchange
access-list CSM_FW_ACL_PARTNER remark Drop all other traffic
access-list CSM_FW_ACL_PARTNER extended deny ip any any log
access-list CSM_FW_ACL_VOICE extended deny ip any object-group Store-MSP-POS-net
access-list CSM_FW_ACL_VOICE extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
access-list CSM_FW_ACL_VOICE extended permit tcp 10.10.176.0 255.255.248.0 object EMC-NCM
eq ssh
access-list CSM_FW_ACL_VOICE extended permit object-group CSM_INLINE_svc_rule_73014461112
10.10.176.0 255.255.248.0 object RSA-enVision
access-list CSM_FW_ACL_VOICE extended permit tcp 10.10.176.0 255.255.248.0 object TACACS
eq tacacs
access-list CSM_FW_ACL_VOICE extended permit udp 10.10.176.0 255.255.248.0 object-group
NTP-Servers eq ntp
access-list CSM_FW_ACL_VOICE extended permit object-group CSM_INLINE_svc_rule_73014461120
10.10.176.0 255.255.248.0 object-group CSM_INLINE_dst_rule_73014461120
access-list CSM_FW_ACL_VOICE remark Voice calls
access-list CSM_FW_ACL_VOICE extended permit object-group CSM_INLINE_svc_rule_73014461130
10.10.178.0 255.255.255.0 object DC-ALL
access-list CSM_FW_ACL_VOICE remark Allow Mail
access-list CSM_FW_ACL_VOICE extended permit object-group CSM_INLINE_svc_rule_73014461138
10.10.176.0 255.255.248.0 object MSExchange
access-list CSM_FW_ACL_VOICE remark Drop all other traffic
access-list CSM_FW_ACL_VOICE extended deny ip any any log
access-list CSM_FW_ACL_WAAS extended deny ip any object-group Store-MSP-POS-net
access-list CSM_FW_ACL_WAAS extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
access-list CSM_FW_ACL_WAAS extended permit tcp 10.10.176.0 255.255.248.0 object EMC-NCM
eq ssh
access-list CSM_FW_ACL_WAAS extended permit object-group CSM_INLINE_svc_rule_73014461112
10.10.176.0 255.255.248.0 object RSA-enVision
access-list CSM_FW_ACL_WAAS extended permit tcp 10.10.176.0 255.255.248.0 object TACACS eq
tacacs
access-list CSM_FW_ACL_WAAS extended permit udp 10.10.176.0 255.255.248.0 object-group
NTP-Servers eq ntp
access-list CSM_FW_ACL_WAAS remark WAAS systems
access-list CSM_FW_ACL_WAAS extended permit object-group CSM_INLINE_svc_rule_73014461132
10.10.184.0 255.255.255.0 object-group DC-WAAS
access-list CSM_FW_ACL_WAAS remark Allow Active Directory Domain
access-list CSM_FW_ACL_WAAS extended permit object-group CSM_INLINE_svc_rule_73014461134
10.10.176.0 255.255.248.0 object ActiveDirectory.cisco-irn.com
access-list CSM_FW_ACL_WAAS remark Drop all other traffic
access-list CSM_FW_ACL_WAAS extended deny ip any any log
access-list CSM_FW_ACL_WIRELESS extended deny ip any object-group Store-MSP-POS-net
access-list CSM_FW_ACL_WIRELESS extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
access-list CSM_FW_ACL_WIRELESS extended permit udp 10.10.176.0 255.255.248.0 object-group
NTP-Servers eq ntp
access-list CSM_FW_ACL_WIRELESS remark Allow Active Directory Domain
access-list CSM_FW_ACL_WIRELESS extended permit object-group
CSM_INLINE_svc_rule_73014461134 10.10.176.0 255.255.248.0 object
ActiveDirectory.cisco-irn.com
access-list CSM_FW_ACL_WIRELESS remark Allow Windows Updates
access-list CSM_FW_ACL_WIRELESS extended permit object-group
CSM_INLINE_svc_rule_73014461136 10.10.176.0 255.255.248.0 object MS-Update
access-list CSM_FW_ACL_WIRELESS remark Allow Mail
```

```
access-list CSM_FW_ACL_WIRELESS extended permit object-group
CSM_INLINE_svc_rule_73014461138 10.10.176.0 255.255.248.0 object MSExchange
access-list CSM_FW_ACL_WIRELESS remark Drop all other traffic
access-list CSM_FW_ACL_WIRELESS extended deny ip any any log
access-list CSM_FW_ACL_WIRELESS-CONTROL extended deny ip any object-group
Store-MSP-POS-net
access-list CSM_FW_ACL_WIRELESS-CONTROL extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
access-list CSM_FW_ACL_WIRELESS-CONTROL extended permit tcp 10.10.176.0 255.255.248.0
object EMC-NCM eq ssh
access-list CSM_FW_ACL_WIRELESS-CONTROL extended permit object-group
CSM_INLINE_svc_rule_73014461112 10.10.176.0 255.255.248.0 object RSA-enVision
access-list CSM_FW_ACL_WIRELESS-CONTROL extended permit tcp 10.10.176.0 255.255.248.0
object TACACS eq tacacs
access-list CSM_FW_ACL_WIRELESS-CONTROL extended permit udp 10.10.176.0 255.255.248.0
object-group NTP-Servers eq ntp
access-list CSM_FW_ACL_WIRELESS-CONTROL extended permit object-group
CSM_INLINE_svc_rule_73014461120 10.10.176.0 255.255.248.0 object-group
CSM_INLINE_dst_rule_73014461120
access-list CSM_FW_ACL_WIRELESS-CONTROL remark Wireless control systems
access-list CSM_FW_ACL_WIRELESS-CONTROL extended permit object-group
CSM_INLINE_svc_rule_73014461128 10.10.183.0 255.255.255.0 object-group
CSM_INLINE_dst_rule_73014461128
access-list CSM_FW_ACL_WIRELESS-CONTROL remark Drop all other traffic
access-list CSM_FW_ACL_WIRELESS-CONTROL extended deny ip any any log
access-list CSM_FW_ACL_WIRELESS-GUEST extended deny ip any object-group Store-MSP-POS-net
access-list CSM_FW_ACL_WIRELESS-GUEST extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
access-list CSM_FW_ACL_WIRELESS-GUEST extended permit udp 10.10.176.0 255.255.248.0
object-group NTP-Servers eq ntp
access-list CSM_FW_ACL_WIRELESS-GUEST remark Drop all other traffic
access-list CSM_FW_ACL_WIRELESS-GUEST extended deny ip any any log
pager lines 24
logging enable
logging trap debugging
logging asdm debugging
logging host MSP-WAN 192.168.42.124
mtu MSP-WAN 1500
mtu POS 1500
mtu DATA 1500
mtu VOICE 1500
mtu WIRELESS 1500
mtu WIRELESS-POS 1500
mtu PARTNER 1500
mtu WIRELESS-GUEST 1500
mtu WIRELESS-CONTROL 1500
mtu WAAS 1500
mtu MANAGEMENT 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any MSP-WAN
icmp permit any POS
icmp permit any DATA
icmp permit any VOICE
icmp permit any WIRELESS
icmp permit any WIRELESS-POS
icmp permit any PARTNER
icmp permit any WIRELESS-GUEST
icmp permit any WIRELESS-CONTROL
icmp permit any WAAS
icmp permit any MANAGEMENT
asdm image disk0:/asdm-641.bin
asdm history enable
arp timeout 14400
```

```
access-group OUTSIDE in interface MSP-WAN
access-group CSM_FW_ACL_POS in interface POS
access-group CSM_FW_ACL_DATA in interface DATA
access-group CSM_FW_ACL_VOICE in interface VOICE
access-group CSM_FW_ACL_WIRELESS in interface WIRELESS
access-group CSM_FW_ACL_WIRELESS-POS in interface WIRELESS-POS
access-group CSM_FW_ACL_PARTNER in interface PARTNER
access-group CSM_FW_ACL_WIRELESS-GUEST in interface WIRELESS-GUEST
access-group CSM_FW_ACL_WIRELESS-CONTROL in interface WIRELESS-CONTROL
access-group CSM_FW_ACL_WAAS in interface WAAS
access-group CSM_FW_ACL_MANAGEMENT in interface MANAGEMENT
route MSP-WAN 0.0.0.0 0.0.0.0 10.10.255.11 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (MANAGEMENT) host 192.168.42.131
 key ******
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa authentication ssh console RETAIL LOCAL
aaa accounting ssh console RETAIL
aaa accounting enable console RETAIL
aaa accounting command privilege 15 RETAIL
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
http server enable
http server idle-timeout 15
http server session-timeout 60
http 10.19.151.99 255.255.255.255 MSP-WAN
http 192.168.41.101 255.255.255.255 MSP-WAN
http 192.168.41.102 255.255.255.255 MSP-WAN
http 192.168.42.122 255.255.255.255 MSP-WAN
http 192.168.42.124 255.255.255.255 MSP-WAN
http 192.168.42.133 255.255.255.255 MSP-WAN
http 192.168.42.138 255.255.255.255 MSP-WAN
no snmp-server location
no snmp-server contact
snmp-server community RetailCMOprivate
no snmp-server enable
telnet timeout 5
ssh 10.19.151.99 255.255.255.255 MSP-WAN
ssh 192.168.41.101 255.255.255.255 MSP-WAN
ssh 192.168.41.102 255.255.255.255 MSP-WAN
ssh 192.168.42.122 255.255.255.255 MSP-WAN
ssh 192.168.42.124 255.255.255.255 MSP-WAN
ssh 192.168.42.133 255.255.255.255 MSP-WAN
ssh 192.168.42.138 255.255.255.255 MSP-WAN
ssh timeout 15
ssh version 2
console timeout 15
dhcprelay server 192.168.42.130 MSP-WAN
dhcprelay enable POS
dhcprelay enable DATA
dhcprelay enable VOICE
dhcprelay enable WIRELESS
dhcprelay enable WIRELESS-POS
dhcprelay enable PARTNER
dhcprelay enable WIRELESS-GUEST
dhcprelay enable WIRELESS-CONTROL
dhcprelay timeout 60
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 192.168.62.162 source MSP-WAN
ntp server 192.168.62.161 source MSP-WAN prefer
webvpn
username csmadmin password <removed> encrypted privilege 15
username retail password <removed>  encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
!
!
prompt hostname context
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
password encryption aes
Cryptochecksum:0b5ca833caa61d445ed02aeee4bbf096
: end
```

FWSM-DMZ-1

```
FWSM-RIE-3# sh run
: Saved
:
FWSM Version 4.1(5)
!
hostname FWSM-RIE-3
domain-name cisco-irn.com
enable password <removed>  encrypted
names
dns-guard
!
interface Vlan21
 nameif inside
 security-level 100
 ip address 192.168.21.10 255.255.255.0
!
interface Vlan22
 nameif outside
 security-level 0
 ip address 192.168.22.1 255.255.255.0 standby 192.168.22.2
!
interface Vlan82
 nameif DMZ
 security-level 20
 ip address 192.168.20.25 255.255.255.248 standby 192.168.20.26
!
interface Vlan91
 description LAN Failover Interface
!
interface Vlan92
```

```
 description STATE Failover Interface
!
interface Vlan2305
 nameif EmailSecurityAppliance
 security-level 50
 ip address 192.168.23.65 255.255.255.240 standby 192.168.23.66
!
interface Vlan2306
 nameif EmailSecurityMgrAppliance
 security-level 60
 ip address 192.168.23.81 255.255.255.240 standby 192.168.23.82
!
passwd <removed>  encrypted
ftp mode passive
dns domain-lookup inside
dns name-server 192.168.42.130
same-security-traffic permit inter-interface
object-group icmp-type CSM_INLINE_svc_rule_81604379602.icmp
 description Generated by CS-Manager from service of FirewallRule# 10
(FWSM-DMZ-1_v1/mandatory)
 icmp-object echo
 icmp-object echo-reply
 icmp-object unreachable
object-group network CSM_INLINE_src_rule_81604379520
 description Generated by CS-Manager from src of FirewallRule# 1 (FWSM-DMZ-1_v1/mandatory)
 network-object 192.168.23.68 255.255.255.255
 network-object 192.168.23.84 255.255.255.255
object-group network CSM_INLINE_src_rule_81604379526
 description Generated by CS-Manager from src of FirewallRule# 2 (FWSM-DMZ-1_v1/mandatory)
 network-object 192.168.23.68 255.255.255.255
 network-object 192.168.23.84 255.255.255.255
object-group network RSA-enVision_1
 description RSA EnVision Syslog collector and SIM
 network-object 192.168.42.124 255.255.255.255
object-group network CSM_INLINE_src_rule_81604379528
 description Generated by CS-Manager from src of FirewallRule# 3 (FWSM-DMZ-1_v1/mandatory)
 network-object 192.168.23.68 255.255.255.255
 network-object 192.168.23.84 255.255.255.255
object-group network NTP-Servers
 description NTP Servers
 network-object 192.168.62.161 255.255.255.255
 network-object 162.168.62.162 255.255.255.255
object-group network CSM_INLINE_src_rule_81604379532
 description Generated by CS-Manager from src of FirewallRule# 4 (FWSM-DMZ-1_v1/mandatory)
 network-object 192.168.23.68 255.255.255.255
 network-object 192.168.23.84 255.255.255.255
object-group network TACACS_1
 description Csico Secure ACS server for TACACS and Radius
 network-object 192.168.42.131 255.255.255.255
object-group network AdminStation
 network-object 192.168.41.101 255.255.255.255
object-group network AdminStation2
 network-object 192.168.41.102 255.255.255.255
object-group network CSM_INLINE_src_rule_81604379552
 description Generated by CS-Manager from src of FirewallRule# 5 (FWSM-DMZ-1_v1/mandatory)
 group-object AdminStation
 group-object AdminStation2
object-group network EMC-NCM
 description EMC Network Configuration Manager
 network-object 192.168.42.122 255.255.255.255
object-group network CSManager
 description Cisco Security Manager
 network-object 192.168.42.133 255.255.255.255
object-group network RSA-enVision
```

```
 description RSA EnVision Syslog collector and SIM
 network-object 192.168.42.124 255.255.255.255
object-group network AdminStation3
 network-object 192.168.42.138 255.255.255.255
object-group network AdminStation4-bart
 network-object 10.19.151.99 255.255.255.255
object-group network Admin-Systems
 group-object EMC-NCM
 group-object AdminStation
 group-object AdminStation2
 group-object CSManager
 group-object RSA-enVision
 group-object AdminStation3
 group-object AdminStation4-bart
object-group network DC-ALL
 description All of the Data Center
 network-object 192.168.0.0 255.255.0.0
object-group network Stores-ALL
 description all store networks
 network-object 10.10.0.0 255.255.0.0
object-group network CSM_INLINE_src_rule_81604379580
 description Generated by CS-Manager from src of FirewallRule# 7 (FWSM-DMZ-1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
object-group network CSM_INLINE_src_rule_81604379592
 description Generated by CS-Manager from src of FirewallRule# 8 (FWSM-DMZ-1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
object-group network CSM_INLINE_src_rule_81604379602
 description Generated by CS-Manager from src of FirewallRule# 10
(FWSM-DMZ-1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
object-group network ActiveDirectory.cisco-irn.com
 network-object 192.168.42.130 255.255.255.255
object-group network PAME-DC-1
 network-object 192.168.44.111 255.255.255.255
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 network-object 192.168.42.131 255.255.255.255
object-group network CSM_INLINE_src_rule_81604379688
 description Generated by CS-Manager from src of FirewallRule# 21
(FWSM-DMZ-1_v1/mandatory)
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
object-group network CSM_INLINE_src_rule_81604379690
 description Generated by CS-Manager from src of FirewallRule# 22
(FWSM-DMZ-1_v1/mandatory)
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
object-group network CSM_INLINE_src_rule_81604379692
 description Generated by CS-Manager from src of FirewallRule# 23
(FWSM-DMZ-1_v1/mandatory)
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
object-group service CSM_INLINE_svc_rule_81604379520.tcp tcp
 description Generated by CS-Manager from service of FirewallRule# 1
(FWSM-DMZ-1_v1/mandatory)
 port-object eq smtp
 port-object eq domain
object-group service CSM_INLINE_svc_rule_81604379532 udp
 description Generated by CS-Manager from service of FirewallRule# 4
(FWSM-DMZ-1_v1/mandatory)
 port-object eq 1812
 port-object eq 1813
object-group service CSM_INLINE_svc_rule_81604379556 tcp
 description Generated by CS-Manager from service of FirewallRule# 6
(FWSM-DMZ-1_v1/mandatory)
 port-object eq ssh
 port-object eq https
object-group service CSM_INLINE_svc_rule_81604379580 tcp
 description Generated by CS-Manager from service of FirewallRule# 7
(FWSM-DMZ-1_v1/mandatory)
 port-object eq smtp
 port-object eq https
 port-object eq ssh
object-group service CSM_INLINE_svc_rule_81604379592 tcp
 description Generated by CS-Manager from service of FirewallRule# 8
(FWSM-DMZ-1_v1/mandatory)
 port-object eq https
 port-object eq ssh
object-group service CSM_INLINE_svc_rule_81604379602.tcp tcp
 description Generated by CS-Manager from service of FirewallRule# 10
(FWSM-DMZ-1_v1/mandatory)
 port-object eq www
 port-object eq ftp
 port-object eq https
 port-object eq 8443
 port-object eq 1080
 port-object eq 8080
 port-object eq telnet
 port-object eq ssh
object-group service CSM_INLINE_svc_rule_81604379626.tcp tcp
 description Generated by CS-Manager from service of FirewallRule# 11
(FWSM-DMZ-1_v1/mandatory)
 port-object eq domain
 port-object eq 123
object-group service CSM_INLINE_svc_rule_81604379626.udp udp
 description Generated by CS-Manager from service of FirewallRule# 11
(FWSM-DMZ-1_v1/mandatory)
 port-object eq domain
 port-object eq ntp
object-group service CSM_INLINE_svc_rule_81604379640.tcp tcp
 description Generated by CS-Manager from service of FirewallRule# 13
(FWSM-DMZ-1_v1/mandatory)
 port-object eq ldap
 port-object eq 3268
 port-object eq 3269
 port-object eq ldaps
object-group service CSM_INLINE_svc_rule_81604379680 tcp
 description Generated by CS-Manager from service of FirewallRule# 18
(FWSM-DMZ-1_v1/mandatory)
 port-object eq https
 port-object eq ssh
object-group service vCenter-to-ESX4 tcp
 description Communication from vCetner to ESX hosts
 port-object eq 5989
 port-object eq 8000
 port-object eq 902
 port-object eq 903
object-group service CSM_INLINE_svc_rule_81604380215.tcp tcp
 description Generated by CS-Manager from service of FirewallRule# 25
(FWSM-DMZ-1_v1/mandatory)
 port-object eq 8880
 port-object eq 8444
 port-object eq 5900
 port-object eq 5800
 port-object eq ssh
 port-object eq 3389
 port-object eq 1080
 port-object eq 8080
 port-object eq telnet
 port-object eq 69
 port-object eq www
 port-object eq https
 port-object eq 8443
 group-object vCenter-to-ESX4
access-list Ironport1-in remark Allow main and DNZ
access-list Ironport1-in extended permit udp object-group CSM_INLINE_src_rule_81604379520
any eq domain
access-list Ironport1-in extended permit tcp object-group CSM_INLINE_src_rule_81604379520
any object-group CSM_INLINE_svc_rule_81604379520.tcp
access-list Ironport1-in extended permit udp object-group CSM_INLINE_src_rule_81604379526
object-group RSA-enVision_1 eq syslog
access-list Ironport1-in extended permit udp object-group CSM_INLINE_src_rule_81604379528
object-group NTP-Servers eq ntp
access-list Ironport1-in extended permit udp object-group CSM_INLINE_src_rule_81604379532
object-group TACACS_1 object-group CSM_INLINE_svc_rule_81604379532
access-list From-DMZ extended permit udp 192.168.20.0 255.255.255.0 object-group
RSA-enVision eq syslog
access-list From-DMZ extended permit tcp 192.168.20.0 255.255.255.0 object-group TACACS eq
tacacs
access-list From-DMZ extended permit udp 192.168.20.0 255.255.255.0 object-group
NTP-Servers eq ntp
access-list Ironport2-in remark Allow main and DNZ
access-list Ironport2-in extended permit udp object-group CSM_INLINE_src_rule_81604379520
any eq domain
access-list Ironport2-in extended permit tcp object-group CSM_INLINE_src_rule_81604379520
any object-group CSM_INLINE_svc_rule_81604379520.tcp
access-list Ironport2-in extended permit udp object-group CSM_INLINE_src_rule_81604379526
object-group RSA-enVision_1 eq syslog
access-list Ironport2-in extended permit udp object-group CSM_INLINE_src_rule_81604379528
object-group NTP-Servers eq ntp
access-list Ironport2-in extended permit udp object-group CSM_INLINE_src_rule_81604379532
object-group TACACS_1 object-group CSM_INLINE_svc_rule_81604379532
access-list INSIDE extended permit tcp object-group Admin-Systems 192.168.20.0
255.255.252.0 object-group CSM_INLINE_svc_rule_81604379556
access-list INSIDE remark Allow services for Ironport apps
access-list INSIDE extended permit tcp object-group CSM_INLINE_src_rule_81604379580
192.168.23.64 255.255.255.224 object-group CSM_INLINE_svc_rule_81604379580
access-list INSIDE remark Allow traffic to DMZ
access-list INSIDE extended permit tcp object-group CSM_INLINE_src_rule_81604379592 host
192.168.20.30 object-group CSM_INLINE_svc_rule_81604379592
access-list INSIDE remark - Drop unauthorized traffic to DMZ
access-list INSIDE extended deny ip any 192.168.20.0 255.255.252.0 log
access-list INSIDE remark Allow outbound services for Internet
access-list INSIDE extended permit icmp object-group CSM_INLINE_src_rule_81604379602 any
object-group CSM_INLINE_svc_rule_81604379602.icmp
access-list INSIDE extended permit tcp object-group CSM_INLINE_src_rule_81604379602 any
object-group CSM_INLINE_svc_rule_81604379602.tcp
access-list INSIDE extended permit tcp object-group ActiveDirectory.cisco-irn.com any
object-group CSM_INLINE_svc_rule_81604379626.tcp
access-list INSIDE extended permit udp object-group ActiveDirectory.cisco-irn.com any
object-group CSM_INLINE_svc_rule_81604379626.udp
access-list INSIDE extended permit udp object-group NTP-Servers any eq ntp
access-list INSIDE remark Allow LDAP out LAB test
access-list INSIDE extended permit udp object-group PAME-DC-1 any eq 389 log
access-list INSIDE extended permit tcp object-group PAME-DC-1 any object-group
CSM_INLINE_svc_rule_81604379640.tcp log
access-list INSIDE remark Drop and Log all other traffic - END-OF-LINE
access-list INSIDE extended deny ip any any log
access-list OUTSIDE remark Allow traffic to DMZ e-commerce Server
```

```
access-list OUTSIDE extended permit tcp any host 192.168.20.30 object-group
CSM_INLINE_svc_rule_81604379680
access-list OUTSIDE remark Mail to Ironport
access-list OUTSIDE extended permit tcp any host 192.168.23.68 eq smtp
access-list OUTSIDE remark Remote Access SSL VPN
access-list OUTSIDE extended permit tcp any host 192.168.21.1 eq https
access-list OUTSIDE remark Allow traffic from edge routers - RIE-1
access-list OUTSIDE extended permit udp object-group CSM_INLINE_src_rule_81604379688
object-group RSA-enVision eq syslog
access-list OUTSIDE remark Allow traffic from edge routers - RIE-1
access-list OUTSIDE extended permit tcp object-group CSM_INLINE_src_rule_81604379690
object-group TACACS eq tacacs
access-list OUTSIDE remark Allow traffic from edge routers - RIE-1
access-list OUTSIDE extended permit udp object-group CSM_INLINE_src_rule_81604379692
object-group NTP-Servers eq ntp
access-list OUTSIDE remark Drop all other traffic
access-list OUTSIDE extended deny ip any any log
pager lines 24
logging host inside 192.168.42.124
mtu inside 1500
mtu outside 1500
mtu EmailSecurityAppliance 1500
mtu EmailSecurityMgrAppliance 1500
mtu DMZ 1500
failover
failover lan unit primary
failover lan interface failover Vlan91
failover link statelink Vlan92
failover interface ip failover 192.168.20.13 255.255.255.252 standby 192.168.20.14
failover interface ip statelink 192.168.20.33 255.255.255.252 standby 192.168.20.34
icmp permit any inside
icmp permit any outside
icmp permit any EmailSecurityAppliance
icmp permit any EmailSecurityMgrAppliance
asdm history enable
arp timeout 14400
access-group INSIDE in interface inside
access-group OUTSIDE in interface outside
access-group Ironport1-in in interface EmailSecurityAppliance
access-group Ironport2-in in interface EmailSecurityMgrAppliance
access-group From-DMZ in interface DMZ
route inside 192.168.0.0 255.255.0.0 192.168.21.1 1
route inside 10.10.0.0 255.255.0.0 192.168.21.1 1
route outside 10.10.0.0 255.255.255.0 192.168.22.10 1
route outside 0.0.0.0 0.0.0.0 192.168.22.10 1
route outside 10.10.3.0 255.255.255.0 192.168.22.11 1
route outside 10.10.4.0 255.255.255.0 192.168.22.12 1
route DMZ 192.168.20.0 255.255.255.248 192.168.20.28 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-invite 0:03:00 sip-disconnect 0:02:00
timeout pptp-gre 0:02:00
timeout uauth 0:05:00 absolute
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL host 192.168.42.131
 key ******
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
aaa authentication ssh console RETAIL LOCAL
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa accounting ssh console RETAIL
aaa accounting enable console RETAIL
aaa accounting command privilege 15 RETAIL
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
http server enable
http 10.19.151.99 255.255.255.255 inside
http 192.168.41.101 255.255.255.255 inside
http 192.168.41.102 255.255.255.255 inside
http 192.168.42.122 255.255.255.255 inside
http 192.168.42.124 255.255.255.255 inside
http 192.168.42.133 255.255.255.255 inside
http 192.168.42.138 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no snmp-server enable
service reset no-connection
no service reset connection marked-for-deletion
telnet timeout 5
ssh 10.19.151.99 255.255.255.255 inside
ssh 192.168.41.101 255.255.255.255 inside
ssh 192.168.41.102 255.255.255.255 inside
ssh 192.168.42.122 255.255.255.255 inside
ssh 192.168.42.124 255.255.255.255 inside
ssh 192.168.42.133 255.255.255.255 inside
ssh 192.168.42.138 255.255.255.255 inside
ssh timeout 15
ssh version 2
console timeout 15
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect skinny
  inspect smtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:0ce5577c4093206d7ce2fc0f65139d9d
: end
FWSM-RIE-3#
```

MDS-DC-1-running

```
!Command: show running-config
```

```
!Time: Sun Apr 24 16:47:39 2011

version 5.0(1a)
system default switchport mode F
feature npiv
feature privilege
feature tacacs+
role name default-role
  description This is a system defined role and applies to all users.
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username admin password 5 <removed> role network-admin
username retail password 5 <removed>   role network-admin
username emc-ncm password 5 <removed>   role network-admin
username bart password 5 <removed>   role network-admin
enable secret 5 <removed>

banner motd #WARNING:    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail
****                    **** AUTHORIZED USERS ONLY! ****ANY USE OF THIS COMPUTER NETWORK
SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENTTO MONITORING OF SUCH USE AND TO SUCH
ADDITIONAL MONITORING AS MAY BE NECESSARYTO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM
ADMINISTRATOR OR OTHERREPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY
TIME WITHOUTFURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY
OTHERCRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAWENFORCEMENT
OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.UNAUTHORIZED ACCESS IS A VIOLATION
OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.#

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host MDS-DC-1 192.168.41.51
tacacs-server key 7 “<removed>”
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
aaa group server radius radius
snmp-server user bart network-admin auth md5 <removed>  priv <removed>  localizedkey
snmp-server user admin network-admin auth md5 <removed>  priv <removed>  localizedkey
snmp-server user retail network-admin auth md5 <removed>  priv <removed>  localizedkey
snmp-server user emc-ncm network-admin auth md5 <removed>  priv <removed>  localizedkey
snmp-server host 192.168.41.101 traps version 2c public  udp-port 2162
snmp-server host 192.168.42.121 traps version 3 auth public
no snmp-server enable traps entity entity_mib_change
no snmp-server enable traps entity entity_module_status_change
no snmp-server enable traps entity entity_power_status_change
no snmp-server enable traps entity entity_module_inserted
no snmp-server enable traps entity entity_module_removed
no snmp-server enable traps entity entity_unrecognised_module
no snmp-server enable traps entity entity_fan_status_change
no snmp-server enable traps entity entity_power_out_change
no snmp-server enable traps rf redundancy_framework
ntp server 192.168.62.161
ntp server 192.168.62.162
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable
ip access-list 23 permit ip 127.0.0.1 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.41.101 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.41.102 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.111 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.121 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.122 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.131 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.133 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.138 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 10.19.151.99 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 deny ip any any log-deny
vsan database
  vsan 2 name "Promise-2"
  vsan 10 name "UIM_VSAN_A_10"
fcdomain fcid database
  vsan 1 wwn 50:00:40:20:03:fc:44:6a fcid 0x020000 dynamic
  vsan 1 wwn 50:00:40:21:03:fc:44:6a fcid 0x020001 dynamic
  vsan 1 wwn 21:00:00:e0:8b:19:70:09 fcid 0x020100 area dynamic
  vsan 1 wwn 20:89:00:05:30:00:99:de fcid 0x020200 area dynamic
  vsan 1 wwn 20:8a:00:05:30:00:99:de fcid 0x020300 area dynamic
  vsan 1 wwn 23:00:00:05:30:00:99:e0 fcid 0x020002 dynamic
  vsan 1 wwn 23:01:00:05:30:00:99:e0 fcid 0x020003 dynamic
  vsan 1 wwn 23:02:00:05:30:00:99:e0 fcid 0x020004 dynamic
  vsan 1 wwn 23:03:00:05:30:00:99:e0 fcid 0x020005 dynamic
  vsan 1 wwn 23:04:00:05:30:00:99:e0 fcid 0x020006 dynamic
  vsan 1 wwn 23:05:00:05:30:00:99:e0 fcid 0x020007 dynamic
  vsan 1 wwn 23:06:00:05:30:00:99:e0 fcid 0x020008 dynamic
  vsan 1 wwn 23:07:00:05:30:00:99:e0 fcid 0x020009 dynamic
  vsan 1 wwn 23:08:00:05:30:00:99:e0 fcid 0x02000a dynamic
  vsan 1 wwn 22:02:00:05:30:00:99:e0 fcid 0x02000b dynamic
  vsan 1 wwn 22:04:00:05:30:00:99:e0 fcid 0x02000c dynamic
  vsan 1 wwn 22:06:00:05:30:00:99:e0 fcid 0x02000d dynamic
  vsan 1 wwn 22:08:00:05:30:00:99:e0 fcid 0x02000e dynamic
  vsan 1 wwn 22:0a:00:05:30:00:99:e0 fcid 0x02000f dynamic
  vsan 1 wwn 22:0c:00:05:30:00:99:e0 fcid 0x020010 dynamic
  vsan 1 wwn 10:00:00:00:c9:60:df:80 fcid 0x020011 dynamic
  vsan 1 wwn 23:12:00:05:30:00:99:e0 fcid 0x020012 dynamic
  vsan 1 wwn 23:13:00:05:30:00:99:e0 fcid 0x020013 dynamic
  vsan 1 wwn 23:14:00:05:30:00:99:e0 fcid 0x020014 dynamic
  vsan 1 wwn 23:15:00:05:30:00:99:e0 fcid 0x020015 dynamic
  vsan 1 wwn 23:17:00:05:30:00:99:e0 fcid 0x020016 dynamic
  vsan 1 wwn 23:16:00:05:30:00:99:e0 fcid 0x020017 dynamic
  vsan 1 wwn 23:18:00:05:30:00:99:e0 fcid 0x020018 dynamic
  vsan 1 wwn 23:19:00:05:30:00:99:e0 fcid 0x020019 dynamic
  vsan 1 wwn 11:00:00:00:00:00:00:01 fcid 0x02001a dynamic
  vsan 1 wwn 20:00:00:00:00:00:00:01 fcid 0x02001b dynamic
  vsan 1 wwn 10:00:00:00:c9:77:94:21 fcid 0x02001c dynamic
  vsan 1 wwn 10:00:00:00:c9:77:92:e9 fcid 0x02001d dynamic
  vsan 1 wwn 10:00:00:00:c9:77:dd:bc fcid 0x02001e dynamic
  vsan 1 wwn 20:41:00:05:9b:73:10:c0 fcid 0x02001f dynamic
  vsan 1 wwn 20:41:00:05:9b:73:17:40 fcid 0x020020 dynamic
  vsan 1 wwn 10:00:00:00:c9:77:dc:c3 fcid 0x020021 dynamic
  vsan 1 wwn 10:00:00:00:c9:75:68:c3 fcid 0x020022 dynamic
  vsan 1 wwn 20:4c:00:0d:ec:2d:94:c0 fcid 0x020400 area dynamic
  vsan 1 wwn 20:64:00:0d:ec:2d:94:c0 fcid 0x020500 area dynamic
  vsan 1 wwn 10:00:00:00:c9:77:db:c3 fcid 0x020023 dynamic
  vsan 2 wwn 20:4c:00:0d:ec:2d:94:c0 fcid 0xef0000 area dynamic
  vsan 2 wwn 10:00:00:00:c9:75:68:c3 fcid 0xef0100 dynamic
  vsan 2 wwn 10:00:00:00:c9:77:dc:c3 fcid 0xef0101 dynamic
  vsan 2 wwn 10:00:00:00:c9:77:dd:bc fcid 0xef0102 dynamic
  vsan 2 wwn 10:00:00:00:c9:77:db:c3 fcid 0xef0103 dynamic
  vsan 2 wwn 10:00:00:00:c9:77:92:e9 fcid 0xef0104 dynamic
  vsan 2 wwn 50:06:01:60:46:e0:33:aa fcid 0xef01ef dynamic
  vsan 2 wwn 20:41:00:05:9b:73:10:c0 fcid 0xef0105 dynamic
  vsan 1 wwn 50:06:01:68:46:e0:33:aa fcid 0x0200ef dynamic
  vsan 1 wwn 50:06:01:60:46:e0:33:aa fcid 0x0206ef dynamic
  vsan 2 wwn 20:41:00:05:9b:73:17:40 fcid 0xef0106 dynamic
  vsan 2 wwn 10:00:00:00:c9:77:94:21 fcid 0xef0107 dynamic
  vsan 2 wwn 20:64:00:0d:ec:2d:94:c0 fcid 0xef0200 area dynamic
  vsan 2 wwn 50:06:01:68:46:e0:33:aa fcid 0xef03ef dynamic
  vsan 10 wwn 50:06:01:60:46:e0:33:aa fcid 0xd800ef dynamic
  vsan 10 wwn 20:41:00:05:9b:73:10:c0 fcid 0xd80000 dynamic
  vsan 10 wwn 20:41:00:05:9b:73:17:40 fcid 0xd80001 dynamic
  vsan 10 wwn 10:00:00:00:c9:77:94:21 fcid 0xd80002 dynamic
  vsan 10 wwn 50:06:01:61:46:e0:33:aa fcid 0xd801ef dynamic
  vsan 10 wwn 50:06:01:69:46:e0:33:aa fcid 0xd802ef dynamic
  vsan 10 wwn 20:42:00:05:9b:73:10:c0 fcid 0xd80003 dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:0f fcid 0xd80004 dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:18 fcid 0xd80005 dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:12 fcid 0xd80006 dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:15 fcid 0xd80007 dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:19 fcid 0xd80008 dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:10 fcid 0xd80009 dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:1c fcid 0xd8000a dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:25 fcid 0xd8000b dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:22 fcid 0xd8000c dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:1f fcid 0xd8000d dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:2b fcid 0xd8000e dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:28 fcid 0xd8000f dynamic
vsan database
  vsan 2 interface fc2/1
  vsan 2 interface fc2/2
  vsan 2 interface fc2/3
  vsan 2 interface fc2/4
  vsan 2 interface fc2/5
  vsan 2 interface fc2/6
  vsan 2 interface fc2/7
  vsan 2 interface fc2/8
  vsan 2 interface fc2/9
  vsan 2 interface fc2/10
  vsan 2 interface fc2/11
  vsan 2 interface fc2/12
  vsan 2 interface fc2/13
  vsan 2 interface fc2/14
  vsan 2 interface fc2/15
  vsan 2 interface fc2/16
  vsan 2 interface fc2/17
  vsan 2 interface fc2/18
  vsan 2 interface fc2/19
  vsan 2 interface fc2/20
  vsan 2 interface fc2/21
  vsan 2 interface fc2/22
  vsan 2 interface fc2/23
  vsan 10 interface fc2/24
  vsan 10 interface fc2/25
  vsan 10 interface fc2/26
  vsan 2 interface fc2/27
  vsan 2 interface fc2/28
  vsan 2 interface fc2/29
  vsan 2 interface fc2/30
  vsan 2 interface fc2/31
  vsan 2 interface fc2/32
  vsan 2 interface fc2/33
  vsan 2 interface fc2/34
  vsan 2 interface fc2/35
  vsan 2 interface fc2/36
  vsan 2 interface fc2/37
  vsan 2 interface fc2/38
  vsan 2 interface fc2/39
  vsan 2 interface fc2/40
  vsan 2 interface fc2/41
  vsan 2 interface fc2/42
  vsan 2 interface fc2/43
  vsan 2 interface fc2/44
  vsan 2 interface fc2/45
  vsan 2 interface fc2/46
  vsan 2 interface fc2/47
  vsan 10 interface fc2/48
  vsan 2 interface fc4/1
  vsan 2 interface fc4/2
  vsan 2 interface fc4/3
  vsan 2 interface fc4/4
  vsan 2 interface fc4/5
  vsan 2 interface fc4/6
  vsan 2 interface fc4/7
  vsan 2 interface fc4/8
  vsan 2 interface fc4/9
  vsan 2 interface fc4/10
  vsan 2 interface fc4/11
  vsan 2 interface fc4/12
  vsan 2 interface fc4/13
  vsan 2 interface fc4/14
  vsan 2 interface fc4/15
  vsan 2 interface fc4/16
  vsan 2 interface fc4/17
  vsan 2 interface fc4/18
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
ip default-gateway 192.168.41.1
switchname MDS-DC-1
line vty
  exec-timeout 15
line console
  exec-timeout 15
boot kickstart bootflash:/m9500-sf2ek9-kickstart-mzg.5.0.1a.bin.S4 sup-1
boot system bootflash:/m9500-sf2ek9-mzg.5.0.1a.bin.S4 sup-1
boot kickstart bootflash:/m9500-sf2ek9-kickstart-mzg.5.0.1a.bin.S4 sup-2
boot system bootflash:/m9500-sf2ek9-mzg.5.0.1a.bin.S4 sup-2
interface fc2/12
  switchport speed 4000
  switchport rate-mode shared
interface fc2/11
  switchport rate-mode dedicated
interface fc2/36
  switchport rate-mode dedicated
interface fc2/1
interface fc2/2
interface fc2/3
interface fc2/4
interface fc2/5
interface fc2/6
interface fc2/7
interface fc2/8
interface fc2/9
interface fc2/10
interface fc2/12
  switchport mode FL
interface fc2/13
interface fc2/14
interface fc2/15
interface fc2/16
interface fc2/17
interface fc2/18
interface fc2/19
interface fc2/20
interface fc2/21
interface fc2/22
interface fc2/23
interface fc2/24
interface fc2/25
interface fc2/26
interface fc2/27
interface fc2/28
interface fc2/29
interface fc2/30
interface fc2/31
interface fc2/32
interface fc2/33
interface fc2/34
interface fc2/35
interface fc2/37
interface fc2/38
interface fc2/39
interface fc2/40
interface fc2/41
interface fc2/42
interface fc2/43
interface fc2/44
interface fc2/45
interface fc2/46
interface fc2/47
interface fc2/48
interface fc2/11
  switchport mode auto
interface fc2/36
  switchport mode auto
interface fc4/1
interface fc4/2
interface fc4/3
interface fc4/4
interface fc4/5
interface fc4/6
interface fc4/7
interface fc4/8
interface fc4/9
interface fc4/10
interface fc4/11
interface fc4/12
interface fc4/13
interface fc4/14
interface fc4/15
interface fc4/16
interface fc4/17
interface fc4/18
logging server 192.168.42.121
logging server 192.168.42.124 6
system default zone default-zone permit
system default zone distribute full
zone default-zone permit vsan 2
zone default-zone permit vsan 10
zoneset distribute full vsan 1-2
zoneset distribute full vsan 10
!Full Zone Database Section for vsan 2
zone name global_zone vsan 2
    member pwwn 26:00:00:01:55:35:7e:44
    member pwwn 26:02:00:01:55:35:7e:44
    member pwwn 10:00:00:00:c9:75:68:c3
    member pwwn 10:00:00:00:c9:77:92:e9
    member pwwn 10:00:00:00:c9:77:db:c3
    member pwwn 10:00:00:00:c9:77:dc:c3
    member pwwn 10:00:00:00:c9:77:dd:bc
    member pwwn 21:00:00:1b:32:00:33:0c
    member pwwn 21:00:00:1b:32:00:3a:0c
    member pwwn 21:00:00:1b:32:00:5d:0d
    member pwwn 21:00:00:1b:32:00:5e:0d
    member pwwn 21:00:00:1b:32:00:70:0d
    member pwwn 21:00:00:1b:32:00:ab:0d
    member pwwn 21:00:00:1b:32:80:0b:10
    member pwwn 21:00:00:1b:32:80:52:10
    member pwwn 21:00:00:1b:32:80:da:0f
    member pwwn 21:00:00:1b:32:80:f1:0f

zoneset name promise-2_zs vsan 2
    member global_zone

zoneset activate name promise-2_zs vsan 2
!Full Zone Database Section for vsan 10
zone name UIM_20000025B5011112_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011110_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011112_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011110_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011112_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011110_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011112_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011110_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011115_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011116_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011115_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011116_5006016146E033AA vsan 10
```

```
        member pwwn 20:00:00:25:b5:01:11:16
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B5011115_5006016946E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:15
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011116_5006016946E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:16
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011115_5006016046E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:15
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011116_5006016046E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:16
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B501111A_5006016946E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1a
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011119_5006016946E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:19
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B501111A_5006016146E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1a
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B5011119_5006016146E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:19
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B501111A_5006016846E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1a
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B5011119_5006016846E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:19
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B501111A_5006016046E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1a
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011119_5006016046E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:19
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B501111D_5006016146E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1d
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B501111C_5006016146E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1c
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B501111D_5006016846E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1d
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B501111C_5006016846E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1c
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B501111D_5006016946E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1d
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B501111C_5006016946E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1c
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B501111D_5006016046E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1d
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B501111C_5006016046E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1c
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B501111F_5006016146E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1f
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B5011120_5006016146E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:20
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B501111F_5006016946E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1f
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011120_5006016946E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:20
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B501111F_5006016846E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1f
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B5011120_5006016846E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:20
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B501111F_5006016046E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:1f
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011120_5006016046E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:20
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011123_5006016946E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:23
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011122_5006016946E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:22
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011123_5006016146E033AA vsan 10
        member pwwn 20:00:00:25:b5:01:11:23
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B5011122_5006016146E033AA vsan 10
```

```
    member pwwn 20:00:00:25:b5:01:11:22
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011123_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:23
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011122_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:22
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011123_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:23
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011122_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:22
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011125_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011126_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011125_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011126_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011125_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011126_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011125_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011126_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011129_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:29
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011128_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011129_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:29
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011128_5006016046E033AA vsan 10
```

```
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011129_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:29
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011128_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011129_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:29
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011128_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501112B_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501112C_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501112B_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501112C_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501112B_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501112C_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501112B_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501112C_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:61:46:e0:33:aa

zoneset name UIM_ZONESET_A vsan 10
    member UIM_20000025B5011112_5006016046E033AA
    member UIM_20000025B5011110_5006016046E033AA
    member UIM_20000025B5011112_5006016946E033AA
    member UIM_20000025B5011110_5006016946E033AA
    member UIM_20000025B5011112_5006016846E033AA
    member UIM_20000025B5011110_5006016846E033AA
    member UIM_20000025B5011112_5006016146E033AA
    member UIM_20000025B5011110_5006016146E033AA
    member UIM_20000025B5011115_5006016846E033AA
    member UIM_20000025B5011116_5006016846E033AA
    member UIM_20000025B5011115_5006016146E033AA
    member UIM_20000025B5011116_5006016146E033AA
    member UIM_20000025B5011115_5006016946E033AA
    member UIM_20000025B5011116_5006016946E033AA
    member UIM_20000025B5011115_5006016046E033AA
    member UIM_20000025B5011116_5006016046E033AA
    member UIM_20000025B501111A_5006016946E033AA
    member UIM_20000025B5011119_5006016946E033AA
    member UIM_20000025B501111A_5006016146E033AA
    member UIM_20000025B5011119_5006016146E033AA
    member UIM_20000025B501111A_5006016846E033AA
    member UIM_20000025B5011119_5006016846E033AA
    member UIM_20000025B501111A_5006016046E033AA
    member UIM_20000025B5011119_5006016046E033AA
    member UIM_20000025B501111D_5006016146E033AA
    member UIM_20000025B501111C_5006016146E033AA
    member UIM_20000025B501111D_5006016846E033AA
    member UIM_20000025B501111C_5006016846E033AA
    member UIM_20000025B501111D_5006016946E033AA
    member UIM_20000025B501111C_5006016946E033AA
    member UIM_20000025B501111D_5006016046E033AA
    member UIM_20000025B501111C_5006016046E033AA
    member UIM_20000025B501111F_5006016146E033AA
    member UIM_20000025B5011120_5006016146E033AA
    member UIM_20000025B501111F_5006016946E033AA
    member UIM_20000025B5011120_5006016946E033AA
    member UIM_20000025B501111F_5006016846E033AA
    member UIM_20000025B5011120_5006016846E033AA
    member UIM_20000025B501111F_5006016046E033AA
    member UIM_20000025B5011120_5006016046E033AA
    member UIM_20000025B5011123_5006016946E033AA
    member UIM_20000025B5011122_5006016946E033AA
    member UIM_20000025B5011123_5006016146E033AA
    member UIM_20000025B5011122_5006016146E033AA
    member UIM_20000025B5011123_5006016846E033AA
    member UIM_20000025B5011122_5006016846E033AA
    member UIM_20000025B5011123_5006016046E033AA
    member UIM_20000025B5011122_5006016046E033AA
    member UIM_20000025B5011125_5006016146E033AA
    member UIM_20000025B5011126_5006016146E033AA
    member UIM_20000025B5011125_5006016946E033AA
    member UIM_20000025B5011126_5006016946E033AA
    member UIM_20000025B5011125_5006016846E033AA
    member UIM_20000025B5011126_5006016846E033AA
    member UIM_20000025B5011125_5006016046E033AA
    member UIM_20000025B5011126_5006016046E033AA
    member UIM_20000025B5011129_5006016846E033AA
    member UIM_20000025B5011128_5006016846E033AA
    member UIM_20000025B5011129_5006016046E033AA
    member UIM_20000025B5011128_5006016046E033AA
    member UIM_20000025B5011129_5006016146E033AA
    member UIM_20000025B5011128_5006016146E033AA
    member UIM_20000025B5011129_5006016946E033AA
    member UIM_20000025B5011128_5006016946E033AA
    member UIM_20000025B501112B_5006016946E033AA
    member UIM_20000025B501112C_5006016946E033AA
    member UIM_20000025B501112B_5006016846E033AA
    member UIM_20000025B501112C_5006016846E033AA
    member UIM_20000025B501112B_5006016046E033AA
    member UIM_20000025B501112C_5006016046E033AA
    member UIM_20000025B501112B_5006016146E033AA
    member UIM_20000025B501112C_5006016146E033AA

zoneset activate name UIM_ZONESET_A vsan 10

interface fc2/1
interface fc2/2

interface fc2/3

interface fc2/4

interface fc2/5

interface fc2/6

interface fc2/7

interface fc2/8

interface fc2/9

interface fc2/10

interface fc2/11
  no shutdown

interface fc2/12
  no shutdown

interface fc2/13

interface fc2/14

interface fc2/15

interface fc2/16

interface fc2/17

interface fc2/18

interface fc2/19

interface fc2/20

interface fc2/21

interface fc2/22

interface fc2/23

interface fc2/24
  no shutdown

interface fc2/25
  no shutdown

interface fc2/26
  no shutdown

interface fc2/27

interface fc2/28

interface fc2/29

interface fc2/30
interface fc2/31

interface fc2/32

interface fc2/33

interface fc2/34

interface fc2/35

interface fc2/36
  no shutdown

interface fc2/37
  shutdown

interface fc2/38

interface fc2/39

interface fc2/40

interface fc2/41

interface fc2/42

interface fc2/43

interface fc2/44

interface fc2/45

interface fc2/46

interface fc2/47

interface fc2/48
  no shutdown

interface fc4/1

interface fc4/2

interface fc4/3

interface fc4/4

interface fc4/5

interface fc4/6

interface fc4/7

interface fc4/8

interface fc4/9

interface fc4/10

interface fc4/11

interface fc4/12

interface fc4/13
interface fc4/14

interface fc4/15

interface fc4/16

interface fc4/17

interface fc4/18

interface GigabitEthernet4/1

interface GigabitEthernet4/2

interface GigabitEthernet4/3

interface GigabitEthernet4/4

interface mgmt0
  ip address 192.168.41.51 255.255.255.0
  ip access-group 23 in
no system default switchport shutdown
```

MDS-DC-2-running

```
!Command: show running-config
!Time: Sun Apr 24 16:48:05 2011

version 5.0(4)
system default switchport mode F
feature npiv
feature privilege
feature tacacs+
role name default-role
  description This is a system defined role and applies to all users.
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username admin password 5 <removed>   role network-admin
username retail password 5 <removed>   role network-admin
username emc-ncm password 5 <removed>   role network-admin
username bart password 5 <removed>   role network-admin
enable secret 5 <removed>

banner motd #
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
```

```
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
#

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host MDS-DC-2 192.168.41.52
ip host MDS-DC-2 192.168.41.52
tacacs-server key 7 “<removed>”
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
aaa group server radius radius
snmp-server user bart network-admin auth md5 <removed>  priv <removed> localizedkey
snmp-server user admin network-admin auth md5 <removed> localizedkey
snmp-server user retail network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user emc-ncm network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server host 192.168.41.101 traps version 2c public  udp-port 2162
snmp-server host 192.168.42.121 traps version 3 auth public
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
ntp server 192.168.62.161
ntp server 192.168.62.162
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable
ip access-list 23 permit ip 127.0.0.1 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.41.101 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.41.102 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.111 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.121 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.122 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.131 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.133 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.138 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 10.19.151.99 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 deny ip any any log-deny
vsan database
  vsan 2 name “Promise-2”
  vsan 11 name “UIM_VSAN_B_11”
fcdomain fcid database
  vsan 1 wwn 21:01:00:e0:8b:39:35:58 fcid 0x010000 area dynamic
  vsan 1 wwn 22:03:00:0d:ec:20:2b:40 fcid 0x010100 area dynamic
  vsan 11 wwn 20:41:00:05:9b:73:17:40 fcid 0xd40000 dynamic
  vsan 11 wwn 20:42:00:05:9b:73:17:40 fcid 0xd40001 dynamic
  vsan 1 wwn 21:00:00:e0:8b:19:35:58 fcid 0x010200 area dynamic
  vsan 11 wwn 50:06:01:69:46:e0:33:aa fcid 0xd400ef dynamic
  vsan 11 wwn 50:06:01:68:46:e0:33:aa fcid 0xd401ef dynamic
  vsan 1 wwn 26:01:00:01:55:35:7e:44 fcid 0x010300 dynamic
  vsan 2 wwn 26:01:00:01:55:35:7e:44 fcid 0x890000 dynamic
  vsan 2 wwn 20:64:00:0d:ec:38:76:00 fcid 0x890100 area dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:10 fcid 0xd40002 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:19 fcid 0xd40003 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:13 fcid 0xd40004 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:16 fcid 0xd40005 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:1a fcid 0xd40006 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:12 fcid 0xd40007 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:1d fcid 0xd40008 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:26 fcid 0xd40009 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:23 fcid 0xd4000a dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:20 fcid 0xd4000b dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:2c fcid 0xd4000c dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:29 fcid 0xd4000d dynamic
vsan database
  vsan 11 interface fc2/24
  vsan 11 interface fc2/25
  vsan 11 interface fc2/26
  vsan 11 interface fc2/48
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
ip default-gateway 192.168.41.1
switchname MDS-DC-2
line vty
  session-limit 32
  exec-timeout 15
line console
  exec-timeout 15
boot kickstart bootflash:/m9500-sf2ek9-kickstart-mz.5.0.4.bin sup-1
boot system bootflash:/m9500-sf2ek9-mz.5.0.4.bin sup-1
boot kickstart bootflash:/m9500-sf2ek9-kickstart-mz.5.0.4.bin sup-2
boot system bootflash:/m9500-sf2ek9-mz.5.0.4.bin sup-2
interface fc2/1
interface fc2/2
interface fc2/3
interface fc2/4
interface fc2/5
interface fc2/6
interface fc2/7
interface fc2/8
interface fc2/9
interface fc2/10
interface fc2/11
interface fc2/12
interface fc2/13
interface fc2/14
interface fc2/15
interface fc2/16
interface fc2/17
interface fc2/18
interface fc2/19
interface fc2/20
interface fc2/21
interface fc2/22
interface fc2/23
interface fc2/24
interface fc2/25
interface fc2/26
interface fc2/27
interface fc2/28
interface fc2/29
interface fc2/30
interface fc2/31
interface fc2/32
interface fc2/33
interface fc2/34
interface fc2/35
interface fc2/36
interface fc2/37
interface fc2/38
interface fc2/39
interface fc2/40
interface fc2/41
interface fc2/42
interface fc2/43
interface fc2/44
interface fc2/45
interface fc2/46
interface fc2/47
interface fc2/48
logging server 192.168.42.121
logging server 192.168.42.124 6
system default zone default-zone permit
system default zone distribute full
zone default-zone permit vsan 2
zone default-zone permit vsan 11
zoneset distribute full vsan 1-2
zoneset distribute full vsan 11
!Full Zone Database Section for vsan 2
zone name global_zone vsan 2
zoneset name promise-2_zs vsan 2
    member global_zone

!Full Zone Database Section for vsan 11
zone name UIM_20000025B5011110_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011112_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011110_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011112_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011110_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011112_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011110_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011112_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011116_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011115_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011116_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011115_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011116_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011115_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011116_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011115_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011119_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501111A_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011119_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501111A_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011119_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501111A_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011119_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501111A_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501111D_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1d
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501111C_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1c
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501111D_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1d
```

```
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B501111C_5006016846E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:1c
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B501111D_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:1d
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B501111C_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:1c
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B501111D_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:1d
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B501111C_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:1c
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011120_5006016846E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:20
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B501111F_5006016846E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:1f
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B5011120_5006016146E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:20
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B501111F_5006016146E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:1f
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B5011120_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:20
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B501111F_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:1f
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011120_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:20
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B501111F_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:1f
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011122_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:22
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011123_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:23
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011122_5006016146E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:22
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B5011123_5006016146E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:23
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B5011122_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:22
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011123_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:23
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011122_5006016846E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:22
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B5011123_5006016846E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:23
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B5011126_5006016846E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:26
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B5011125_5006016846E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:25
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B5011126_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:26
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011125_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:25
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011126_5006016146E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:26
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B5011125_5006016146E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:25
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B5011126_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:26
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011125_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:25
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011128_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:28
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011129_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:29
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B5011128_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:28
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011129_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:29
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B5011128_5006016146E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:28
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B5011129_5006016146E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:29
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B5011128_5006016846E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:28
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B5011129_5006016846E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:29
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B501112C_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:2c
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B501112B_5006016046E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:2b
        member pwwn 50:06:01:60:46:e0:33:aa

    zone name UIM_20000025B501112C_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:2c
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B501112B_5006016946E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:2b
        member pwwn 50:06:01:69:46:e0:33:aa

    zone name UIM_20000025B501112C_5006016846E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:2c
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B501112B_5006016846E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:2b
        member pwwn 50:06:01:68:46:e0:33:aa

    zone name UIM_20000025B501112C_5006016146E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:2c
        member pwwn 50:06:01:61:46:e0:33:aa

    zone name UIM_20000025B501112B_5006016146E033AA vsan 11
        member pwwn 20:00:00:25:b5:01:11:2b
        member pwwn 50:06:01:61:46:e0:33:aa

    zoneset name UIM_ZONESET_B vsan 11
        member UIM_20000025B5011110_5006016946E033AA
        member UIM_20000025B5011112_5006016946E033AA
        member UIM_20000025B5011110_5006016046E033AA
        member UIM_20000025B5011112_5006016046E033AA
        member UIM_20000025B5011110_5006016146E033AA
        member UIM_20000025B5011112_5006016146E033AA
        member UIM_20000025B5011110_5006016846E033AA
        member UIM_20000025B5011112_5006016846E033AA
        member UIM_20000025B5011116_5006016046E033AA
        member UIM_20000025B5011115_5006016046E033AA
        member UIM_20000025B5011116_5006016946E033AA
        member UIM_20000025B5011115_5006016946E033AA
        member UIM_20000025B5011116_5006016846E033AA
        member UIM_20000025B5011115_5006016846E033AA
        member UIM_20000025B5011116_5006016146E033AA
        member UIM_20000025B5011115_5006016146E033AA
        member UIM_20000025B5011119_5006016146E033AA
        member UIM_20000025B501111A_5006016146E033AA
        member UIM_20000025B5011119_5006016046E033AA
        member UIM_20000025B501111A_5006016046E033AA
        member UIM_20000025B5011119_5006016946E033AA
        member UIM_20000025B501111A_5006016946E033AA
        member UIM_20000025B5011119_5006016846E033AA
        member UIM_20000025B501111A_5006016846E033AA
        member UIM_20000025B501111D_5006016146E033AA
        member UIM_20000025B501111C_5006016146E033AA
        member UIM_20000025B501111D_5006016846E033AA
        member UIM_20000025B501111C_5006016846E033AA
        member UIM_20000025B501111D_5006016946E033AA
        member UIM_20000025B501111C_5006016946E033AA
        member UIM_20000025B501111D_5006016046E033AA
        member UIM_20000025B501111C_5006016046E033AA
        member UIM_20000025B5011120_5006016846E033AA
        member UIM_20000025B501111F_5006016846E033AA
        member UIM_20000025B5011120_5006016146E033AA
        member UIM_20000025B501111F_5006016146E033AA
        member UIM_20000025B5011120_5006016046E033AA
        member UIM_20000025B501111F_5006016046E033AA
        member UIM_20000025B5011120_5006016946E033AA
        member UIM_20000025B501111F_5006016946E033AA
        member UIM_20000025B5011122_5006016946E033AA
        member UIM_20000025B5011123_5006016946E033AA
        member UIM_20000025B5011122_5006016146E033AA
        member UIM_20000025B5011123_5006016146E033AA
        member UIM_20000025B5011122_5006016046E033AA
        member UIM_20000025B5011123_5006016046E033AA
        member UIM_20000025B5011122_5006016846E033AA
        member UIM_20000025B5011123_5006016846E033AA
        member UIM_20000025B5011126_5006016846E033AA
        member UIM_20000025B5011125_5006016846E033AA
        member UIM_20000025B5011126_5006016946E033AA
        member UIM_20000025B5011125_5006016946E033AA
        member UIM_20000025B5011126_5006016146E033AA
        member UIM_20000025B5011125_5006016146E033AA
        member UIM_20000025B5011126_5006016046E033AA
        member UIM_20000025B5011125_5006016046E033AA
        member UIM_20000025B5011128_5006016946E033AA
        member UIM_20000025B5011129_5006016946E033AA
        member UIM_20000025B5011128_5006016046E033AA
        member UIM_20000025B5011129_5006016046E033AA
        member UIM_20000025B5011128_5006016146E033AA
        member UIM_20000025B5011129_5006016146E033AA
        member UIM_20000025B5011128_5006016846E033AA
        member UIM_20000025B5011129_5006016846E033AA
        member UIM_20000025B501112C_5006016046E033AA
        member UIM_20000025B501112B_5006016046E033AA
        member UIM_20000025B501112C_5006016946E033AA
        member UIM_20000025B501112B_5006016946E033AA
        member UIM_20000025B501112C_5006016846E033AA
        member UIM_20000025B501112B_5006016846E033AA
        member UIM_20000025B501112C_5006016146E033AA
        member UIM_20000025B501112B_5006016146E033AA
```

```
zoneset activate name UIM_ZONESET_B vsan 11

interface fc2/1

interface fc2/2

interface fc2/3

interface fc2/4

interface fc2/5

interface fc2/6

interface fc2/7

interface fc2/8

interface fc2/9

interface fc2/10

interface fc2/11

interface fc2/12

interface fc2/13

interface fc2/14

interface fc2/15

interface fc2/16

interface fc2/17

interface fc2/18

interface fc2/19

interface fc2/20

interface fc2/21

interface fc2/22

interface fc2/23

interface fc2/24

interface fc2/25

interface fc2/26

interface fc2/27

interface fc2/28

interface fc2/29

interface fc2/30

interface fc2/31
interface fc2/32

interface fc2/33

interface fc2/34

interface fc2/35

interface fc2/36

interface fc2/37

interface fc2/38

interface fc2/39

interface fc2/40

interface fc2/41

interface fc2/42

interface fc2/43

interface fc2/44

interface fc2/45

interface fc2/46

interface fc2/47

interface fc2/48

interface mgmt0
  ip address 192.168.41.52 255.255.255.0
  ip access-group 23 in
no system default switchport shutdown
```

N1kv-1-running

```
!Command: show running-config
!Time: Sat Apr 30 03:02:54 2011

version 4.2(1)SV1(4)
no feature telnet
feature tacacs+

username admin password 5 <removed>   role network-admin
username retail password 5 <removed>   role network-admin

banner motd #
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
```

```
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
#

ssh key rsa 2048
ip domain-lookup
ip domain-lookup
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
hostname N1kv-1
ip access-list 23
  10 permit ip 192.168.42.0/24 any
  20 permit ip any any
  30 deny ip any any
ip access-list 88
  10 permit ip 192.168.42.0/24 any
  20 permit ip any any
  30 deny ip any any
vem 3
  host vmware id 414e3537-3441-3255-5838-34353034544b
vem 4
  host vmware id 414e3537-3441-3255-5838-34353034544d
vem 5
  host vmware id 414e3537-3441-3255-5838-333930345046
vem 6
  host vmware id 414e3537-3441-3255-5838-34353034544c
vem 7
  host vmware id 414e3537-3441-3255-5838-333930344e59
vem 8
  host vmware id 414e3537-3441-3255-5838-333830333330
vem 9
  host vmware id 414e3537-3441-3255-5838-333930345057
vem 10
  host vmware id 414e3537-3441-3255-5838-343530345630
vem 11
  host vmware id 414e3537-3441-3255-5838-343530345448
vem 12
  host vmware id 414e3537-3441-3255-5838-333930345048
snmp-server user admin network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user retail network-admin auth md5 <removed> priv <removed> localizedkey
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management
ntp source 192.168.41.61
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS

vrf context management
  ip route 0.0.0.0/0 192.168.41.1
vlan 1
vlan 36
  name VLAN36
vlan 37
  name VLAN37
vlan 38
  name VLAN38
```

```
vlan 39
  name VLAN39
vlan 40
  name VLAN40
vlan 41
  name VLAN41
vlan 42
  name VLAN42
vlan 43
  name VLAN43
vlan 44
  name VLAN44
vlan 45
  name VLAN45
vlan 46
  name VLAN46
vlan 52
  name VLAN52
vlan 64
  name VLAN64
vlan 72
  name VLAN72
vlan 80
  name VLAN80
vlan 81
  name VLAN81
vlan 82
  name VLAN82
vlan 83
  name VLAN83
port-channel load-balance ethernet source-mac
port-profile default max-ports 32
port-profile type vethernet VLAN38
  vmware port-group
  switchport mode access
  switchport access vlan 38
  no shutdown
  state enabled
port-profile type vethernet VLAN36
  vmware port-group
  switchport mode access
  switchport access vlan 36
  no shutdown
  state enabled
port-profile type vethernet VLAN37
  vmware port-group
  switchport mode access
  switchport access vlan 37
  no shutdown
  state enabled
port-profile type vethernet VLAN39
  vmware port-group
  switchport mode access
  switchport access vlan 39
  no shutdown
  state enabled
port-profile type vethernet VLAN40
  vmware port-group
  switchport mode access
  switchport access vlan 40
  no shutdown
  state enabled
port-profile type vethernet VLAN41
  vmware port-group
  switchport mode access
  switchport access vlan 41
  no shutdown
  system vlan 41
  state enabled
port-profile type vethernet VLAN42
  vmware port-group
  switchport mode access
  switchport access vlan 42
  no shutdown
  state enabled
port-profile type vethernet VLAN43
  vmware port-group
  switchport mode access
  switchport access vlan 43
  no shutdown
  state enabled
port-profile type vethernet VLAN44
  vmware port-group
  switchport mode access
  switchport access vlan 44
  no shutdown
  state enabled
port-profile type vethernet VLAN45
  vmware port-group
  switchport mode access
  switchport access vlan 45
  no shutdown
  state enabled
port-profile type vethernet VLAN46
  vmware port-group
  switchport mode access
  switchport access vlan 46
  no shutdown
  state enabled
port-profile type vethernet VLAN52
  vmware port-group
  switchport mode access
  switchport access vlan 52
  no shutdown
  state enabled
port-profile type vethernet VLAN64
  vmware port-group
  switchport mode access
  switchport access vlan 64
  no shutdown
  state enabled
port-profile type vethernet VLAN72
  vmware port-group
  switchport mode access
  switchport access vlan 72
  no shutdown
  state enabled
port-profile type vethernet VLAN80
  vmware port-group
  switchport mode access
  switchport access vlan 80
  no shutdown
  state enabled
port-profile type vethernet VLAN81
  vmware port-group
  switchport mode access
  switchport access vlan 81
  no shutdown
  state enabled
port-profile type vethernet VLAN82
  vmware port-group
  switchport mode access
  switchport access vlan 82
  no shutdown
  state enabled
port-profile type vethernet VLAN83
  vmware port-group
  switchport mode access
  switchport access vlan 83
  no shutdown
  state enabled
port-profile type ethernet Unused_Or_Quarantine_Uplink
  vmware port-group
  shutdown
  description Port-group created for Nexus1000V internal usage. Do not use.
  state enabled
port-profile type vethernet Unused_Or_Quarantine_Veth
  vmware port-group
  shutdown
  description Port-group created for Nexus1000V internal usage. Do not use.
  state enabled
port-profile type ethernet sysuplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 36-83
  no shutdown
  system vlan 41
  state enabled
port-profile type vethernet VSG-DADA-HA
  vmware port-group
  switchport access vlan 41
  no shutdown
  state enabled
port-profile type vethernet Tenant-1
  vmware port-group
  org root/Tenant-1
  vn-service ip-address 192.168.52.11 vlan 52 security-profile SecurityProfile-1
  switchport mode access
  switchport access vlan 41
  no shutdown
  state enabled

vdc N1kv-1 id 1
  limit-resource vlan minimum 16 maximum 2049
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 32 maximum 32
  limit-resource u6route-mem minimum 16 maximum 16
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

interface mgmt0
  ip address 192.168.41.61/24

interface Vethernet3
  inherit port-profile VLAN42
  description RSA-Archer,Network Adapter 1
  vmware dvport 207 dvswitch uuid "f9 31 3b 50 f5 23 1c a3-34 b1 f1 a6 d6 24 6c c0"
  vmware vm mac 0050.56BB.001E

interface Vethernet5
```

```
  inherit port-profile VSG-DADA-HA
  description Nexus1000VSG,Network Adapter 3
  vmware dvport 1057 dvswitch uuid "f9 31 3b 50 f5 23 1c a3-34 b1 f1 a6 d6 24 6c c0"
  vmware vm mac 0050.56BB.0004

interface Vethernet6
  inherit port-profile VSG-DADA-HA
  description Nexus1000VSG,Network Adapter 1
  vmware dvport 1056 dvswitch uuid "f9 31 3b 50 f5 23 1c a3-34 b1 f1 a6 d6 24 6c c0"
  vmware vm mac 0050.56BB.0002

interface Vethernet7
  inherit port-profile VLAN52
  description POS Terminal,Network Adapter 1
  vmware dvport 352 dvswitch uuid "f9 31 3b 50 f5 23 1c a3-34 b1 f1 a6 d6 24 6c c0"
  vmware vm mac 0050.56BB.0005

interface control0
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
line vty
  exec-timeout 15
line console
  exec-timeout 15
boot kickstart bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.4.bin sup-1
boot system bootflash:/nexus-1000v-mz.4.2.1.SV1.4.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.4.bin sup-2
boot system bootflash:/nexus-1000v-mz.4.2.1.SV1.4.bin sup-2
svs-domain
  domain id 2
  control vlan 41
  packet vlan 41
  svs mode L2
svs connection vc
  protocol vmware-vim
  remote ip address 192.168.41.102 port 80
  vmware dvs uuid "f9 31 3b 50 f5 23 1c a3-34 b1 f1 a6 d6 24 6c c0" datacenter-name Retail
Lab-CMO
  connect
vnm-policy-agent
  registration-ip 192.168.41.65
  shared-secret **********
  policy-agent-image bootflash:/vnmc-vsmpa.1.0.1j.bin
  log-level
logging server 192.168.42.124 7 facility syslog
logging timestamp milliseconds
```

r-a2-conv-1

```
!
! Last configuration change at 00:53:21 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 00:53:22 PST Sat Apr 30 2011 by retail
!
```

```
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
no service password-recovery
!
hostname R-A2-Conv-1
!
boot-start-marker
boot system flash c890-universalk9-mz.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PST recurring
service-module wlan-ap 0 bootimage autonomous
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-479252603
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-479252603
 revocation-check none
 rsakeypair TP-self-signed-479252603
!
!
crypto pki certificate chain TP-self-signed-479252603
 certificate self-signed 01
  <removed>
```

```
    quit
no ip source-route
!
!
!
!
!
ip cef
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip multicast-routing
ip port-map user-8443 port tcp 8443
ip ips config location flash: retries 1 timeout 1
ip ips name Store-IPS
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
ip inspect log drop-pkt
ip inspect audit-trail
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
parameter-map type inspect Inspect-1
 audit-trail on
parameter-map type inspect global
 WAAS enable

parameter-map type trend-global trend-glob-map
password encryption aes
license udi pid CISCO891W-AGN-N-K9 sn <removed>
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
```

```
object-group network Stores-ALL
 description all store networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_68719541425
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for stores
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_68719541431
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_68719541435
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_68719541457
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_68719541461
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_68719541465
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
```

```
object-group network CSM_INLINE_dst_rule_73014451187
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_73014451193
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_73014451223
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_68719541409
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network CSM_INLINE_src_rule_68719541427
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_src_rule_68719541429
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_68719541433
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
```

```
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_68719541437
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_73014451215
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_73014451217
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group service CSM_INLINE_svc_rule_68719541409
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_68719541425
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_68719541427
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
```

```
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_68719541429
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_68719541431
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_68719541437
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_68719541439
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_68719541455
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
```

```
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_68719541457
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_68719541459
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group service CSM_INLINE_svc_rule_73014451187
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_73014451193
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_73014451195
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_73014451197
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_73014451203
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_73014451205
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
```

```
!
object-group service CSM_INLINE_svc_rule_73014451207
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_73014451209
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_73014451211
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_73014451213
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_73014451215
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_73014451217
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
```

```
object-group service CSM_INLINE_svc_rule_73014451221
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_73014451223
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_73014451388
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_73014451393
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_73014451395
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451397
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451404
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451406
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group network DC-Applications
 description Applications in the Data Center that are non-PCI related(Optimized by
CS-Manager)
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network STORE-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
!
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
```

```
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url "*SalesReport*"
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
```

```
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map type inspect CSM_ZBF_POLICY_S_Security_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Data_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Data-W_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAN_S_Guest
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAN_S_Data-W
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Voice_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Guest_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_MGMT_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_LOOPBACK_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_POS-W
 class class-default
  drop log
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_Partners
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_POS
 class class-default
  drop log
```

```
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
```

```
   inspect Inspect-1
  class class-default
   drop
 policy-map type inspect CSM_ZBF_POLICY_MAP_17
  class type inspect CSM_ZBF_CLASS_MAP_25
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_26
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_27
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_15
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_16
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_19
   inspect Inspect-1
  class class-default
   drop
 policy-map type inspect CSM_ZBF_POLICY_MAP_14
  class type inspect CSM_ZBF_CLASS_MAP_22
   inspect Inspect-1
  class class-default
   drop
 policy-map type inspect CSM_ZBF_POLICY_MAP_15
  class type inspect CSM_ZBF_CLASS_MAP_13
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_14
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_15
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_16
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_17
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_23
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_12
  class type inspect CSM_ZBF_CLASS_MAP_13
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_14
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_15
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_16
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_19
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_17
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_20
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_21
  class type inspect CSM_ZBF_CLASS_MAP_15
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_16
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_19
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_17
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_30
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_34
   drop log
  class type inspect CSM_ZBF_CLASS_MAP_35
   inspect Inspect-1
  class class-default
   drop
 policy-map type inspect CSM_ZBF_POLICY_S_MGMT_S_POS
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_13
  class type inspect CSM_ZBF_CLASS_MAP_13
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_14
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_15
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_16
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_17
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_21
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_20
  class type inspect CSM_ZBF_CLASS_MAP_15
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_16
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_19
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_17
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_32
   drop log
  class type inspect CSM_ZBF_CLASS_MAP_33
   inspect Inspect-1
  class class-default
   drop
 policy-map type inspect CSM_ZBF_POLICY_MAP_10
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_11
  class type inspect CSM_ZBF_CLASS_MAP_13
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_14
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_18
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_15
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_16
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_17
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_22
  class type inspect CSM_ZBF_CLASS_MAP_15
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_16
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_19
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_17
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_36
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_S_Voice_S_POS-W
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_S_Guest_S_POS-W
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_9
  class type inspect CSM_ZBF_CLASS_MAP_13
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_14
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_15
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_16
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_17
   inspect Inspect-1
  class class-default
   drop
 policy-map type inspect CSM_ZBF_POLICY_MAP_8
  class type inspect CSM_ZBF_CLASS_MAP_3
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_12
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_7
  class type inspect CSM_ZBF_CLASS_MAP_9
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_10
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_11
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_6
  class type inspect CSM_ZBF_CLASS_MAP_6
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_3
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_5
  class type inspect CSM_ZBF_CLASS_MAP_1
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_3
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_8
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_4
  class type inspect CSM_ZBF_CLASS_MAP_1
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_6
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_3
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_7
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_3
  class type inspect CSM_ZBF_CLASS_MAP_1
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_3
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_5
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_2
  class type inspect CSM_ZBF_CLASS_MAP_1
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_4
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_3
   inspect Inspect-1
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_MAP_1
  class type inspect CSM_ZBF_CLASS_MAP_1
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_2
   inspect Inspect-1
  class type inspect CSM_ZBF_CLASS_MAP_3
   inspect Inspect-1
  class class-default
   drop
 policy-map type inspect CSM_ZBF_POLICY_S_Partners_S_POS
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_S_Security_S_POS
  class class-default
   drop log
 policy-map BRANCH-LAN-EDGE-IN
  class BRANCH-MISSION-CRITICAL
   set ip dscp 25
  class BRANCH-TRANSACTIONAL-DATA
   set ip dscp af21
  class BRANCH-NET-MGMT
   set ip dscp cs2
  class BRANCH-BULK-DATA
   set ip dscp af11
  class BRANCH-SCAVENGER
   set ip dscp cs1
 policy-map type inspect CSM_ZBF_POLICY_S_Data_S_POS
  class class-default
   drop log
 policy-map type inspect CSM_ZBF_POLICY_S_Data-W_S_POS-W
  class class-default
   drop log
 !
 zone security S_WAN
  description Store WAN Link
 zone security LOOPBACK
  description Loopback interface
 zone security S_MGMT
  description VLAN1000 Management
 zone security S_Security
```

```
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_S_WAN_S_Data-W
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_S_WAN_S_Guest
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_LOOPBACK_S_POS-W
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_MGMT_S_POS
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_MGMT_S_POS-W
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Security_S_POS
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Security_S_POS-W
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
```

```
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_POS
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_POS-W
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_Partners
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS-W
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Data_S_POS
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Data_S_POS-W
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Data-W_S_POS
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Data-W_S_POS-W
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Guest_S_POS
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Guest_S_POS-W
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Partners_S_POS
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Voice_S_POS
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Voice_S_POS-W
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.174.1 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface FastEthernet0
```

```
 switchport mode trunk
!
interface FastEthernet1
 switchport access vlan 17
 switchport protected
!
interface FastEthernet2
 switchport access vlan 17
 switchport protected
!
interface FastEthernet3
 switchport access vlan 17
 switchport protected
!
interface FastEthernet4
 switchport access vlan 17
 switchport protected
!
interface FastEthernet5
 switchport access vlan 17
 switchport protected
!
interface FastEthernet6
 switchport access vlan 17
 switchport protected
!
interface FastEthernet7
 switchport access vlan 17
 switchport protected
!
interface FastEthernet8
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet8.1
!
interface GigabitEthernet0
 ip address 10.10.255.160 255.255.255.0
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface wlan-ap0
 description Service module interface to manage the embedded AP
 ip address 10.10.174.33 255.255.255.252
 zone-member security S_WLC-AP
 service-module ip address 10.10.174.34 255.255.255.252
 service-module ip default-gateway 10.10.174.33
 arp timeout 0
!
interface Wlan-GigabitEthernet0
 description Internal switch interface connecting to the embedded AP
 switchport mode trunk
 zone-member security S_WLC-AP
 service-module ip address 10.10.174.34 255.255.255.252
 service-module ip default-gateway 10.10.174.33
!
interface Vlan1
 no ip address
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
!
interface Vlan11
 description POS
 ip address 10.10.160.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
 standby 11 ip 10.10.160.1
 standby 11 priority 101
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan12
 description DATA
 ip address 10.10.161.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.161.1
 standby 12 priority 101
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan13
 description VOICE
 ip address 10.10.162.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.162.1
 standby 13 priority 101
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan14
 description WIRELESS
 ip address 10.10.163.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.163.1
 standby 14 priority 101
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan15
 description WIRELESS-POS
 ip address 10.10.164.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS-W
 standby 15 ip 10.10.164.1
 standby 15 priority 101
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan16
 description PARTNER
 ip address 10.10.165.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.165.1
 standby 16 priority 101
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan17
 description WIRELESS-GUEST
 ip address 10.10.166.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.166.1
 standby 17 priority 101
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan18
 description WIRELESS-CONTROL
 ip address 10.10.167.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.167.1
 standby 18 priority 101
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan19
 description WAAS
 ip address 10.10.168.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.168.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan20
 description SECURITY
 ip address 10.10.169.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Security
 standby 20 ip 10.10.169.1
 standby 20 priority 101
 standby 20 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan1000
 description MANAGEMENT
 ip address 10.10.175.2 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.175.1
 standby 100 priority 101
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Async1
 no ip address
 encapsulation slip
!
interface Group-Async0
 physical-layer async
 no ip address
 encapsulation slip
 no group-range
!
router ospf 5
 router-id 10.10.174.1
 passive-interface default
!
no ip forward-protocol nd
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip route 0.0.0.0 0.0.0.0 10.10.255.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_68719541409 object-group 
CSM_INLINE_src_rule_68719541409 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451205 object-group DC-POS-Oracle 
object-group STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451209 object-group DC-POS-SAP object-group 
STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451213 object-group DC-POS-Tomax 
object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451215 object-group 
CSM_INLINE_src_rule_73014451215 object-group STORE-POS
```

```
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_68719541455 object-group DC-Voice object-group 
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_73014451187 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_73014451187
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_73014451193 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_73014451193
ip access-list extended CSM_ZBF_CMAP_ACL_15
 remark Store to Data Center for NTP
 permit object-group NTP object-group Stores-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_73014451221 object-group Stores-ALL object-group 
ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541425 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_68719541425
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store UCS Express to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_73014451197 object-group Stores-ALL object-group 
vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_73014451223 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_73014451223
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Stores-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Store to Data Center Physical Security
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_68719541435
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_68719541439 object-group Stores-ALL object-group 
DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_73014451388 object-group Stores-ALL object-group 
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_68719541431 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_68719541431
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451203 object-group STORE-POS object-group 
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451207 object-group STORE-POS object-group 
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451211 object-group STORE-POS object-group 
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451217 object-group 
CSM_INLINE_src_rule_73014451217 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_26
```

```
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451393 object-group STORE-POS object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451395 object-group STORE-POS object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Permit POS clients to talk to store POS server
 permit object-group CSM_INLINE_svc_rule_73014451397 object-group STORE-POS object-group
STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451404 object-group Stores-ALL object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541427 object-group
CSM_INLINE_src_rule_68719541427 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451406 object-group Stores-ALL object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_68719541459 object-group Stores-ALL object-group
DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_68719541465
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_68719541461
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_68719541457 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_68719541457
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS Express
 permit object-group CSM_INLINE_svc_rule_73014451195 object-group vSphere-1 object-group
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_68719541433 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_68719541437 object-group
CSM_INLINE_src_rule_68719541437 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP's and Controllers in stores
 permit object-group CSM_INLINE_svc_rule_68719541429 object-group
CSM_INLINE_src_rule_68719541429 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group STORE-POS
```

```
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large store Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group causer v3 priv
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps energywise
snmp-server enable traps config-copy
```

```
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line 1
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
line 2
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication RETAIL
 no exec
 transport preferred none
 transport output none
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
scheduler max-task-time 5000
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

r-a2-lrg-1

```
!
! Last configuration change at 00:54:49 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 00:54:49 PST Sat Apr 30 2011 by retail
!
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname R-A2-Lrg-1
!
boot-start-marker
boot system flash0 c3900-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
```

```
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PST recurring
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-72006796
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-72006796
 revocation-check none
!
!
crypto pki certificate chain TP-self-signed-72006796
 certificate self-signed 03
  <removed>
    quit
no ipv6 cef
no ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip port-map user-8443 port tcp 8443
ip inspect log drop-pkt
ip inspect audit-trail
ip ips config location flash0: retries 1 timeout 1
ip ips name Store-IPS
```

```
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
!
parameter-map type inspect global
 WAAS enable
parameter-map type inspect Inspect-1
 audit-trail on

parameter-map type trend-global trend-glob-map
!
!
!
!
password encryption aes
voice-card 0
!
!
!
!
!
!
!
license udi pid C3900-SPE150/K9 sn <removed>
hw-module pvdm 0/0
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
```

```
!
object-group network CSM_INLINE_dst_rule_81604380995
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_81604381001
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_81604381037
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Stores-ALL
 description all store networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_81604381039
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for stores
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_81604381045
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_81604381049
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_81604381059
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_81604381067
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_81604381071
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_81604381150
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_dst_rule_81604381152
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_81604380993
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_81604381021
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381023
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381041
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_src_rule_81604381043
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_81604381047
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_81604381051
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network CSM_INLINE_src_rule_81604381150
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_src_rule_81604381152
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group service CSM_INLINE_svc_rule_81604380993
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_81604380995
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_81604381001
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_81604381003
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_81604381005
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_81604381009
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_81604381011
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service CSM_INLINE_svc_rule_81604381013
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381015
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_81604381017
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_81604381019
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_81604381021
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
```

```
!
object-group service CSM_INLINE_svc_rule_81604381023
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381025
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_81604381027
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381029
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_81604381035
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_81604381037
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381039
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_81604381041
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_81604381043
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_81604381045
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_81604381051
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381053
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381055
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381057
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_81604381059
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service CSM_INLINE_svc_rule_81604381061
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381063
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_81604381065
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group network DC-Applications
 description Applications in the Data Center that are non-PCI related(Optimized by
CS-Manager)
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network STORE-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
redundancy
!
!
!
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
```

```
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_37
 match access-group name CSM_ZBF_CMAP_ACL_37
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
```

```
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
```

```
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_38
 match access-group name CSM_ZBF_CMAP_ACL_38
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
```

```
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url "*SalesReport*"
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_MAP_18
```

```
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_25
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_37
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_24
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_27
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_26
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_38
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_15
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_23
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
```

```
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
!
zone security S_WAN
 description Store WAN Link
zone security S_R-2-R
 description Bridge link between routers
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
```

```
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_S_R-2-R-LOOPBACK_1 source S_R-2-R destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_R-2-R-S_MGMT_1 source S_R-2-R destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_R-2-R-S_Security_1 source S_R-2-R destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_R-2-R-S_WAAS_1 source S_R-2-R destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_R-2-R-S_WLC-AP_1 source S_R-2-R destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_R-2-R-self_1 source S_R-2-R destination self
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_S_R-2-R-S_Data_1 source S_R-2-R destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Data-W_1 source S_R-2-R destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Guest_1 source S_R-2-R destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_R-2-R-S_Partners_1 source S_R-2-R destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_POS_1 source S_R-2-R destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_POS-W_1 source S_R-2-R destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_Voice_1 source S_R-2-R destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_self-S_R-2-R_1 source self destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_R-2-R_1 source LOOPBACK destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
```

```
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_R-2-R_1 source S_MGMT destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_R-2-R_1 source S_Security destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_R-2-R_1 source S_WAAS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_R-2-R_1 source S_WLC-AP destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-S_R-2-R_1 source S_POS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_R-2-R_1 source S_POS-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-S_R-2-R_1 source S_Data destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
```

```
zone-pair security CSM_S_Data-W-S_R-2-R_1 source S_Data-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Guest-S_R-2-R_1 source S_Guest destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Partners-S_R-2-R_1 source S_Partners destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_26
zone-pair security CSM_S_Voice-S_R-2-R_1 source S_Voice destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_27
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.110.1 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface GigabitEthernet0/0
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.96.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip helper-address 192.168.42.111
 ip pim sparse-dense-mode
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
 standby 11 ip 10.10.96.1
 standby 11 priority 101
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.97.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.97.1
 standby 12 priority 101
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.98.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.98.1
 standby 13 priority 101
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.14
 description WIRELESS
 encapsulation dot1Q 14
 ip address 10.10.99.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.99.1
 standby 14 priority 101
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.100.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS-W
 standby 15 ip 10.10.100.1
 standby 15 priority 101
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.101.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.101.1
 standby 16 priority 101
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.17
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.102.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.102.1
 standby 17 priority 101
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.103.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.103.1
 standby 18 priority 101
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.19
 description WAAS
 encapsulation dot1Q 19
 ip address 10.10.104.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.104.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.20
 description SECURITY-SYSTEMS
 encapsulation dot1Q 20
 ip address 10.10.105.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Security
 standby 20 ip 10.10.105.1
 standby 20 priority 101
 standby 20 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.102
 description ROUTER LINK TO
 encapsulation dot1Q 102
 ip address 10.10.110.29 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
interface GigabitEthernet0/0.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.111.2 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.111.1
 standby 100 priority 101
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
```

```
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.101
 description ROUTER LINK TO
 encapsulation dot1Q 101
 ip address 10.10.110.25 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
interface GigabitEthernet0/2
 ip address 10.10.255.96 255.255.255.0
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
!
router ospf 5
 router-id 10.10.110.1
 redistribute connected subnets
 passive-interface default
 no passive-interface GigabitEthernet0/0.102
 no passive-interface GigabitEthernet0/1.101
 network 10.10.0.0 0.0.255.255 area 10
 default-information originate
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.10.255.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_81604380993 object-group
CSM_INLINE_src_rule_81604380993 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381011 object-group DC-POS-Oracle
object-group STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381015 object-group DC-POS-SAP object-group
STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381019 object-group DC-POS-Tomax
object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381021 object-group
CSM_INLINE_src_rule_81604381021 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_81604381057 object-group DC-Voice object-group
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 permit ospf object-group CSM_INLINE_src_rule_81604381150 object-group
CSM_INLINE_dst_rule_81604381150
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_81604381055 object-group Stores-ALL object-group
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_15
 permit ospf object-group CSM_INLINE_src_rule_81604381152 object-group
CSM_INLINE_dst_rule_81604381152
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_81604380995 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604380995
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_81604381001 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381001
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store to Data Center for NTP
 permit object-group NTP object-group Stores-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_81604381035 object-group Stores-ALL object-group
ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Stores-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381039 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381039
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store UCS Express to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_81604381005 object-group Stores-ALL object-group
vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_81604381037 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381037
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center Physical Security
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381049
ip access-list extended CSM_ZBF_CMAP_ACL_24
```

```
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_81604381053 object-group Stores-ALL object-group
DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_81604381045 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381045
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381009 object-group STORE-POS object-group
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381013 object-group STORE-POS object-group
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381017 object-group STORE-POS object-group
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381023 object-group
CSM_INLINE_src_rule_81604381023 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381025 object-group STORE-POS object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381027 object-group STORE-POS object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381041 object-group
CSM_INLINE_src_rule_81604381041 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Permit POS clients to talk to store POS server
 permit object-group CSM_INLINE_svc_rule_81604381029 object-group STORE-POS object-group
STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381061 object-group Stores-ALL object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381063 object-group Stores-ALL object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_81604381065 object-group Stores-ALL object-group
DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381071
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381067
ip access-list extended CSM_ZBF_CMAP_ACL_37
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_38
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_81604381059 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381059
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS Express
 permit object-group CSM_INLINE_svc_rule_81604381003 object-group vSphere-1 object-group
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_81604381047 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_81604381051 object-group
CSM_INLINE_src_rule_81604381051 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP's and Controllers in stores
 permit object-group CSM_INLINE_svc_rule_81604381043 object-group
CSM_INLINE_src_rule_81604381043 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group STORE-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large store Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
```

```
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
banner exec C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
```

```
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication RETAIL
 no exec
 transport preferred none
 transport output none
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

r-a2-lrg-2

```
!
! Last configuration change at 00:59:26 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:00:56 PST Sat Apr 30 2011 by retail
!
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname R-A2-Lrg-2
!
boot-start-marker
boot system flash0 c3900-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PST recurring
!
crypto pki token default removal timeout 0
```

```
!
crypto pki trustpoint TP-self-signed-660084654
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-660084654
 revocation-check none
 rsakeypair TP-self-signed-660084654
!
!
crypto pki certificate chain TP-self-signed-660084654
 certificate self-signed 01
  <removed>
    quit
no ipv6 cef
no ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip port-map user-8443 port tcp 8443
ip inspect log drop-pkt
ip inspect audit-trail
ip ips config location flash0: retries 1 timeout 1
ip ips name Store-IPS
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
!
parameter-map type inspect global
 WAAS enable
parameter-map type inspect Inspect-1
 audit-trail on

parameter-map type trend-global trend-glob-map
!
!
!
!
password encryption aes
voice-card 0
!
!
!
!
!
!
!
```

```
license udi pid C3900-SPE150/K9 sn <removed>
hw-module pvdm 0/0
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_81604380995
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_81604381001
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_81604381037
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Stores-ALL
 description all store networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_81604381039
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for stores
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_81604381045
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_81604381049
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_81604381059
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_81604381067
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_81604381071
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_81604381150
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_dst_rule_81604381152
```

```
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_81604380993
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_81604381021
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381023
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381041
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_src_rule_81604381043
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_81604381047
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_81604381051
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network CSM_INLINE_src_rule_81604381150
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_src_rule_81604381152
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group service CSM_INLINE_svc_rule_81604380993
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_81604380995
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_81604381001
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_81604381003
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_81604381005
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
```

```
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_81604381009
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_81604381011
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service CSM_INLINE_svc_rule_81604381013
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381015
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
```

```
!
object-group service CSM_INLINE_svc_rule_81604381017
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_81604381019
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_81604381021
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381023
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381025
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_81604381027
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381029
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service DNS-Resolving
```

```
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_81604381035
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_81604381037
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381039
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_81604381041
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_81604381043
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
```

```
!
object-group service CSM_INLINE_svc_rule_81604381045
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_81604381051
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381053
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381055
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381057
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_81604381059
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service CSM_INLINE_svc_rule_81604381061
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381063
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
```

```
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_81604381065
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group network DC-Applications
 description Applications in the Data Center that are non-PCI related(Optimized by
CS-Manager)
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network STORE-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
redundancy
!
!
!
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
```

```
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
```

```
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_37
 match access-group name CSM_ZBF_CMAP_ACL_37
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_38
 match access-group name CSM_ZBF_CMAP_ACL_38
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url “*SalesReport*”
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
```

```
!
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
```

```
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_25
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_37
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_24
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_27
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_16
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_26
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_38
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_15
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_23
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
!
zone security S_WAN
 description Store WAN Link
zone security S_R-2-R
 description Bridge link between routers
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_S_R-2-R-LOOPBACK_1 source S_R-2-R destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_R-2-R-S_MGMT_1 source S_R-2-R destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_R-2-R-S_Security_1 source S_R-2-R destination S_Security
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_R-2-R-S_WAAS_1 source S_R-2-R destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_R-2-R-S_WLC-AP_1 source S_R-2-R destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_R-2-R-self_1 source S_R-2-R destination self
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_S_R-2-R-S_Data_1 source S_R-2-R destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Data-W_1 source S_R-2-R destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Guest_1 source S_R-2-R destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_R-2-R-S_Partners_1 source S_R-2-R destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_POS_1 source S_R-2-R destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_POS-W_1 source S_R-2-R destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_Voice_1 source S_R-2-R destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_self-S_R-2-R_1 source self destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_R-2-R_1 source LOOPBACK destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_R-2-R_1 source S_MGMT destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_R-2-R_1 source S_Security destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_R-2-R_1 source S_WAAS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_R-2-R_1 source S_WLC-AP destination S_R-2-R
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-S_R-2-R_1 source S_POS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_R-2-R_1 source S_POS-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-S_R-2-R_1 source S_Data destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_R-2-R_1 source S_Data-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Guest-S_R-2-R_1 source S_Guest destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Partners-S_R-2-R_1 source S_Partners destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_26
zone-pair security CSM_S_Voice-S_R-2-R_1 source S_Voice destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_27
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.110.2 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.102
 description ROUTER LINK TO
 encapsulation dot1Q 102
 ip address 10.10.110.30 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
!
interface GigabitEthernet0/1
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.96.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
 standby 11 ip 10.10.96.1
 standby 11 priority 99
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.97.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.97.1
 standby 12 priority 99
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.98.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.98.1
 standby 13 priority 99
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
```

```
interface GigabitEthernet0/1.14
 description WIRELESS
 encapsulation dot1Q 14
 ip address 10.10.99.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.99.1
 standby 14 priority 99
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.100.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS-W
 standby 15 ip 10.10.100.1
 standby 15 priority 99
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.101.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.101.1
 standby 16 priority 99
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.17
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.102.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.102.1
 standby 17 priority 99
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.103.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.103.1
 standby 18 priority 99
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.19
 description WAAS
 encapsulation dot1Q 19
 ip address 10.10.104.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.104.1
 standby 19 priority 99
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.20
 description SECURITY-SYSTEMS
 encapsulation dot1Q 20
 ip address 10.10.105.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Security
 standby 20 ip 10.10.105.1
 standby 20 priority 99
 standby 20 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.101
 description ROUTER LINK TO
 encapsulation dot1Q 101
 ip address 10.10.110.26 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
!
interface GigabitEthernet0/1.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.111.3 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.111.1
 standby 100 priority 99
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/2
 ip address 10.10.254.96 255.255.255.0
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
!
router ospf 5
 router-id 10.10.110.2
 redistribute connected subnets
 passive-interface default
 no passive-interface GigabitEthernet0/0.102
 no passive-interface GigabitEthernet0/1.101
 network 10.10.0.0 0.0.255.255 area 10
 default-information originate
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.10.254.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_81604380993 object-group 
CSM_INLINE_src_rule_81604380993 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381011 object-group DC-POS-Oracle 
object-group STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381015 object-group DC-POS-SAP object-group 
STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381019 object-group DC-POS-Tomax 
object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381021 object-group 
CSM_INLINE_src_rule_81604381021 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_81604381057 object-group DC-Voice object-group 
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 permit ospf object-group CSM_INLINE_src_rule_81604381150 object-group 
CSM_INLINE_dst_rule_81604381150
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_81604381055 object-group Stores-ALL object-group 
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_15
 permit ospf object-group CSM_INLINE_src_rule_81604381152 object-group 
CSM_INLINE_dst_rule_81604381152
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_81604380995 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_81604380995
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_81604381001 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381001
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store to Data Center for NTP
 permit object-group NTP object-group Stores-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_81604381035 object-group Stores-ALL object-group
ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Stores-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381039 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381039
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store UCS Express to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_81604381005 object-group Stores-ALL object-group
vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_81604381037 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381037
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center Physical Security
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381049
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_81604381053 object-group Stores-ALL object-group
DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_81604381045 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381045
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381009 object-group STORE-POS object-group
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381013 object-group STORE-POS object-group
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381017 object-group STORE-POS object-group
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381023 object-group
CSM_INLINE_src_rule_81604381023 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381025 object-group STORE-POS object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381027 object-group STORE-POS object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381041 object-group
CSM_INLINE_src_rule_81604381041 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Permit POS clients to talk to store POS server
 permit object-group CSM_INLINE_svc_rule_81604381029 object-group STORE-POS object-group
STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381061 object-group Stores-ALL object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381063 object-group Stores-ALL object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_81604381065 object-group Stores-ALL object-group
DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381071
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381067
ip access-list extended CSM_ZBF_CMAP_ACL_37
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_38
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_81604381059 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381059
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS Express
 permit object-group CSM_INLINE_svc_rule_81604381003 object-group vSphere-1 object-group
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_81604381047 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_81604381051 object-group
CSM_INLINE_src_rule_81604381051 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP's and Controllers in stores
 permit object-group CSM_INLINE_svc_rule_81604381043 object-group
CSM_INLINE_src_rule_81604381043 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group STORE-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large store Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
```

```
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
banner exec C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication RETAIL
 no exec
 transport preferred none
 transport output none
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

r-a2-med-1

```
!
! Last configuration change at 00:29:32 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 00:29:32 PSTDST Sat Apr 30 2011 by retail
!
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname R-A2-Med-1
!
boot-start-marker
boot system flash0 c2951-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
```

```
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
memory-size iomem 25
clock timezone PST -8 0
clock summer-time PSTDST recurring
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1670063162
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1670063162
 revocation-check none
 rsakeypair TP-self-signed-1670063162
!
!
crypto pki certificate chain TP-self-signed-1670063162
 certificate self-signed 01
  <removed>
    quit
no ipv6 cef
no ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip inspect audit-trail
ip ips config location ipstest retries 1 timeout 1
ip ips notify SDEE
ip ips name Retail-PCI
!
ip ips signature-category
  category all
   retired true
  category ios_ips basic
   retired false
!
```

```
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
!
parameter-map type inspect global
 WAAS enable
parameter-map type inspect Inspect-1
 audit-trail on

parameter-map type trend-global trend-glob-map
!
!
!
!
password encryption aes
voice-card 0
!
!
!
!
!
!
!
license udi pid STARSCREAM sn <removed>
hw-module pvdm 0/2
!
hw-module sm 1
!
hw-module sm 2
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_81604380995
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_81604381001
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_81604381037
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Stores-ALL
 description all store networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_81604381039
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for stores
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_81604381045
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
```

```
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_81604381049
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_81604381059
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_81604381067
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_81604381071
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_81604381150
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_dst_rule_81604381152
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_81604380993
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_81604381021
```

```
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381023
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381041
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_src_rule_81604381043
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_81604381047
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_81604381051
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network CSM_INLINE_src_rule_81604381150
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_src_rule_81604381152
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group service CSM_INLINE_svc_rule_81604380993
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_81604380995
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
```

```
object-group service CSM_INLINE_svc_rule_81604381001
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_81604381003
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_81604381005
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_81604381009
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_81604381011
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service CSM_INLINE_svc_rule_81604381013
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381015
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_81604381017
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_81604381019
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_81604381021
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381023
```

```
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381025
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_81604381027
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381029
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_81604381035
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_81604381037
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381039
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_81604381041
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_81604381043
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_81604381045
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_81604381051
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381053
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
```

```
!
object-group service CSM_INLINE_svc_rule_81604381055
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381057
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_81604381059
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service CSM_INLINE_svc_rule_81604381061
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381063
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_81604381065
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group network DC-Applications
 description Applications in the Data Center that are non-PCI related(Optimized by 
CS-Manager)
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network STORE-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
!
redundancy
!
!
!
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
```

```
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_37
 match access-group name CSM_ZBF_CMAP_ACL_37
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_38
 match access-group name CSM_ZBF_CMAP_ACL_38
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url "*SalesReport*"
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
```

```
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_25
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_37
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class class-default
```

```
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_24
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_27
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_26
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_38
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_15
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_21
```

```
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_23
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
```

```
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
!
zone security S_WAN
 description Store WAN Link
zone security S_R-2-R
 description Bridge link between routers
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
```

```
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_S_R-2-R-LOOPBACK_1 source S_R-2-R destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_R-2-R-S_MGMT_1 source S_R-2-R destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_R-2-R-S_Security_1 source S_R-2-R destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_R-2-R-S_WAAS_1 source S_R-2-R destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_R-2-R-S_WLC-AP_1 source S_R-2-R destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_R-2-R-self_1 source S_R-2-R destination self
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_S_R-2-R-S_Data_1 source S_R-2-R destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Data-W_1 source S_R-2-R destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Guest_1 source S_R-2-R destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_R-2-R-S_Partners_1 source S_R-2-R destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_POS_1 source S_R-2-R destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_POS-W_1 source S_R-2-R destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_Voice_1 source S_R-2-R destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_self-S_R-2-R_1 source self destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_R-2-R_1 source LOOPBACK destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_R-2-R_1 source S_MGMT destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_R-2-R_1 source S_Security destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_R-2-R_1 source S_WAAS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_R-2-R_1 source S_WLC-AP destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-S_R-2-R_1 source S_POS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_R-2-R_1 source S_POS-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-S_R-2-R_1 source S_Data destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_R-2-R_1 source S_Data-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Guest-S_R-2-R_1 source S_Guest destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Partners-S_R-2-R_1 source S_Partners destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_26
zone-pair security CSM_S_Voice-S_R-2-R_1 source S_Voice destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_27
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.126.1 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface GigabitEthernet0/0
 ip address 10.10.255.112 255.255.255.0
 ip ips Retail-PCI in
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface GigabitEthernet0/1
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.112.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_POS
 standby 11 ip 10.10.112.1
 standby 11 priority 101
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
```

```
interface GigabitEthernet0/1.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.113.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.113.1
 standby 12 priority 101
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.114.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.114.1
 standby 13 priority 101
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.14
 description WIRELESS
 encapsulation dot1Q 14
 ip address 10.10.115.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.115.1
 standby 14 priority 101
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.116.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_POS-W
 standby 15 ip 10.10.116.1
 standby 15 priority 101
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.117.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.117.1
 standby 16 priority 101
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.17
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.118.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.118.1
 standby 17 priority 101
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.119.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.119.1
 standby 18 priority 101
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.19
 description WAAS
 encapsulation dot1Q 19
 ip address 10.10.120.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.120.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.20
 description SECURITY-SYSTEMS
 encapsulation dot1Q 20
 ip address 10.10.121.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Security
 standby 20 ip 10.10.121.1
 standby 20 priority 101
 standby 20 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.102
 description ROUTER LINK TO
 encapsulation dot1Q 102
 ip address 10.10.126.29 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
interface GigabitEthernet0/1.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.127.2 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.127.1
 standby 100 priority 101
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
```

```
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/2.101
 description ROUTER LINK TO
 encapsulation dot1Q 101
 ip address 10.10.126.25 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
interface SM1/0
 ip address 10.10.126.41 255.255.255.252
 zone-member security S_WAAS
 service-module fail-open
 service-module ip address 10.10.126.42 255.255.255.252
 service-module ip default-gateway 10.10.126.41
 hold-queue 60 out
!
interface SM1/1
 description Internal switch interface connected to Service Module
!
interface Vlan1
 no ip address
!
!
router ospf 5
 router-id 10.10.126.1
 redistribute connected subnets
 passive-interface default
 no passive-interface GigabitEthernet0/1.102
 no passive-interface GigabitEthernet0/2.101
 network 10.10.0.0 0.0.255.255 area 10
 default-information originate
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.10.255.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_81604380993 object-group
CSM_INLINE_src_rule_81604380993 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381011 object-group DC-POS-Oracle
object-group STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381015 object-group DC-POS-SAP object-group
STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381019 object-group DC-POS-Tomax
object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381021 object-group
CSM_INLINE_src_rule_81604381021 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_81604381057 object-group DC-Voice object-group
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 permit ospf object-group CSM_INLINE_src_rule_81604381150 object-group
CSM_INLINE_dst_rule_81604381150
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_81604381055 object-group Stores-ALL object-group
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_15
 permit ospf object-group CSM_INLINE_src_rule_81604381152 object-group
CSM_INLINE_dst_rule_81604381152
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_81604380995 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604380995
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_81604381001 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381001
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store to Data Center for NTP
 permit object-group NTP object-group Stores-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_81604381035 object-group Stores-ALL object-group
ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Stores-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381039 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381039
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store UCS Express to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_81604381005 object-group Stores-ALL object-group
vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_81604381037 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381037
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center Physical Security
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381049
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_81604381053 object-group Stores-ALL object-group
DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_81604381045 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381045
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381009 object-group STORE-POS object-group
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381013 object-group STORE-POS object-group
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381017 object-group STORE-POS object-group
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381023 object-group
CSM_INLINE_src_rule_81604381023 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381025 object-group STORE-POS object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381027 object-group STORE-POS object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381041 object-group
CSM_INLINE_src_rule_81604381041 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Permit POS clients to talk to store POS server
 permit object-group CSM_INLINE_svc_rule_81604381029 object-group STORE-POS object-group
STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381061 object-group Stores-ALL object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381063 object-group Stores-ALL object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_81604381065 object-group Stores-ALL object-group
DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381071
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381067
```

```
ip access-list extended CSM_ZBF_CMAP_ACL_37
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_38
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_81604381059 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381059
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS Express
 permit object-group CSM_INLINE_svc_rule_81604381003 object-group vSphere-1 object-group
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_81604381047 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_81604381051 object-group
CSM_INLINE_src_rule_81604381051 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP's and Controllers in stores
 permit object-group CSM_INLINE_svc_rule_81604381043 object-group
CSM_INLINE_src_rule_81604381043 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group STORE-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large store Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
```

```
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
mgcp fax t38 ecm
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
banner exec C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
```

```
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY




!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication RETAIL
 no exec
 transport preferred none
 transport output none
line 67
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
```

```
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

r-a2-med-2

```
!
! Last configuration change at 23:30:34 PCTime Fri Apr 29 2011 by retail
! NVRAM config last updated at 23:30:35 PCTime Fri Apr 29 2011 by retail
!
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname R-A2-MED-2
!
boot-start-marker
boot system flash:c2951-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 500000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
clock timezone PCTime -8 0
clock summer-time PCTime date Apr 6 2003 2:00 Oct 26 2003 2:00
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-104836678
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-104836678
 revocation-check none
!
!
crypto pki certificate chain TP-self-signed-104836678
 certificate self-signed 02
  <removed>
    quit
no ipv6 cef
no ip source-route
no ip gratuitous-arps
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip port-map user-8443 port tcp 8443
ip ips notify SDEE
ip ips name Retail-PCI
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
!
parameter-map type inspect global
 WAAS enable
parameter-map type inspect Inspect-1
 audit-trail on
```

```
parameter-map type trend-global trend-glob-map
!
!
!
!
password encryption aes
voice-card 0
!
!
!
!
!
!
!
license udi pid CISCO2951/K9 sn <removed>
hw-module sm 1
!
hw-module sm 2
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_81604380995
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
```

```
object-group network CSM_INLINE_dst_rule_81604381001
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_81604381037
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Stores-ALL
 description all store networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_81604381039
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for stores
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_81604381045
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_81604381049
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_81604381059
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
```

```
!
object-group network CSM_INLINE_dst_rule_81604381067
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_81604381071
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_81604381150
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_dst_rule_81604381152
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_81604380993
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_81604381021
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381023
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381041
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_src_rule_81604381043
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_81604381047
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_81604381051
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network CSM_INLINE_src_rule_81604381150
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_src_rule_81604381152
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group service CSM_INLINE_svc_rule_81604380993
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_81604380995
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_81604381001
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
```

```
!
object-group service CSM_INLINE_svc_rule_81604381003
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_81604381005
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_81604381009
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_81604381011
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service HTTPS-8443
 tcp eq 8443
!
```

```
object-group service CSM_INLINE_svc_rule_81604381013
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381015
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_81604381017
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_81604381019
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_81604381021
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381023
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381025
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_81604381027
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381029
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_81604381035
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_81604381037
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381039
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_81604381041
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
```

```
object-group service CSM_INLINE_svc_rule_81604381043
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_81604381045
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_81604381051
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381053
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381055
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381057
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-HA_v1/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_81604381059
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service CSM_INLINE_svc_rule_81604381061
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381063
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_81604381065
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group network DC-Applications
 description Applications in the Data Center that are non-PCI related(Optimized by
CS-Manager)
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
```

```
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network STORE-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
redundancy
!
!
!
!
ip tcp synwait-time 10
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
```

```
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_19
```

```
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_37
 match access-group name CSM_ZBF_CMAP_ACL_37
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
```

```
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_38
 match access-group name CSM_ZBF_CMAP_ACL_38
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
```

```
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url “*SalesReport*”
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_25
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_37
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_24
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_27
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_26
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_38
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_15
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
```

```
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_23
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
!
zone security S_WAN
 description Store WAN Link
zone security S_R-2-R
 description Bridge link between routers
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_S_R-2-R-LOOPBACK_1 source S_R-2-R destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_R-2-R-S_MGMT_1 source S_R-2-R destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_R-2-R-S_Security_1 source S_R-2-R destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_R-2-R-S_WAAS_1 source S_R-2-R destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_R-2-R-S_WLC-AP_1 source S_R-2-R destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_R-2-R-self_1 source S_R-2-R destination self
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_S_R-2-R-S_Data_1 source S_R-2-R destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Data-W_1 source S_R-2-R destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Guest_1 source S_R-2-R destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_R-2-R-S_Partners_1 source S_R-2-R destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_POS_1 source S_R-2-R destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_POS-W_1 source S_R-2-R destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_Voice_1 source S_R-2-R destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_self-S_R-2-R_1 source self destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_R-2-R_1 source LOOPBACK destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_R-2-R_1 source S_MGMT destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_R-2-R_1 source S_Security destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_R-2-R_1 source S_WAAS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_R-2-R_1 source S_WLC-AP destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-S_R-2-R_1 source S_POS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_R-2-R_1 source S_POS-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-S_R-2-R_1 source S_Data destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_R-2-R_1 source S_Data-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Guest-S_R-2-R_1 source S_Guest destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Partners-S_R-2-R_1 source S_Partners destination S_R-2-R
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_26
zone-pair security CSM_S_Voice-S_R-2-R_1 source S_Voice destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_27
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.126.2 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface GigabitEthernet0/0
 ip address 10.10.254.112 255.255.255.0
 ip ips Retail-PCI in
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface GigabitEthernet0/1
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.112.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_POS
 standby 11 ip 10.10.112.1
 standby 11 priority 99
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.113.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.113.1
 standby 12 priority 99
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
```

```
interface GigabitEthernet0/1.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.114.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.114.1
 standby 13 priority 99
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.14
 description WIRELESS
 encapsulation dot1Q 14
 ip address 10.10.115.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.115.1
 standby 14 priority 99
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.116.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_POS-W
 standby 15 ip 10.10.116.1
 standby 15 priority 99
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.117.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.117.1
 standby 16 priority 99
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.17
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.118.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.118.1
 standby 17 priority 99
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.119.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.119.1
 standby 18 priority 99
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.19
 description WAAS
 encapsulation dot1Q 19
 ip address 10.10.120.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.120.1
 standby 19 priority 99
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.20
 description SECURITY-SYSTEMS
 encapsulation dot1Q 20
 ip address 10.10.121.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Security
 standby 20 ip 10.10.121.1
 standby 20 priority 99
 standby 20 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.101
 description ROUTER LINK TO
 encapsulation dot1Q 101
 ip address 10.10.126.26 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
interface GigabitEthernet0/1.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.127.3 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.127.1
 standby 100 priority 99
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/2.102
 description ROUTER LINK TO
 encapsulation dot1Q 102
 ip address 10.10.126.30 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
```

```
interface SM1/0
 description Video Survillance VMSS Module
 ip address 10.10.126.45 255.255.255.252
 zone-member security S_Security
 service-module ip address 10.10.126.46 255.255.255.252
 !Application: FNDN Running on SM
 service-module ip default-gateway 10.10.126.45
 hold-queue 60 out
!
interface SM1/1
 description Internal switch interface connected to Service Module
!
interface SM2/0
 ip address 10.10.126.50 255.255.255.252
 zone-member security S_MGMT
 service-module ip address 10.10.126.49 255.255.255.252
 !Application: SRE-V Running on SMV
 service-module ip default-gateway 10.10.126.50
 service-module mgf ip address 10.10.125.49 255.255.255.0
 hold-queue 60 out
!
interface SM2/1
 description Internal switch interface connected to Service Module
!
interface Vlan1
 description ESXi Host and Virtual Machines$ES_LAN$
 ip address 10.10.125.50 255.255.255.0
 zone-member security S_POS
!
!
router ospf 5
 router-id 10.10.126.2
 redistribute connected subnets
 passive-interface default
 no passive-interface GigabitEthernet0/1.101
 no passive-interface GigabitEthernet0/2.102
 network 10.10.0.0 0.0.255.255 area 10
 default-information originate
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.10.254.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_81604380993 object-group
CSM_INLINE_src_rule_81604380993 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381011 object-group DC-POS-Oracle
object-group STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381015 object-group DC-POS-SAP object-group
STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381019 object-group DC-POS-Tomax
object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381021 object-group
CSM_INLINE_src_rule_81604381021 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_81604381057 object-group DC-Voice object-group
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 permit ospf object-group CSM_INLINE_src_rule_81604381150 object-group
CSM_INLINE_dst_rule_81604381150
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_81604381055 object-group Stores-ALL object-group
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_15
 permit ospf object-group CSM_INLINE_src_rule_81604381152 object-group
CSM_INLINE_dst_rule_81604381152
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_81604380995 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604380995
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_81604381001 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381001
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store to Data Center for NTP
 permit object-group NTP object-group Stores-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_81604381035 object-group Stores-ALL object-group
ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Stores-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381039 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_81604381039
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store UCS Express to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_81604381005 object-group Stores-ALL object-group
vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_81604381037 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_81604381037
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center Physical Security
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381049
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_81604381053 object-group Stores-ALL object-group 
DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_81604381045 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_81604381045
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381009 object-group STORE-POS object-group 
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381013 object-group STORE-POS object-group 
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381017 object-group STORE-POS object-group 
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381023 object-group 
CSM_INLINE_src_rule_81604381023 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381025 object-group STORE-POS object-group 
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381027 object-group STORE-POS object-group 
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381041 object-group 
CSM_INLINE_src_rule_81604381041 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Permit POS clients to talk to store POS server
 permit object-group CSM_INLINE_svc_rule_81604381029 object-group STORE-POS object-group 
STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381061 object-group Stores-ALL object-group 
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381063 object-group Stores-ALL object-group 
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_81604381065 object-group Stores-ALL object-group 
DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381071
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_81604381067
```

```
ip access-list extended CSM_ZBF_CMAP_ACL_37
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_38
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_81604381059 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_81604381059
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS Express
 permit object-group CSM_INLINE_svc_rule_81604381003 object-group vSphere-1 object-group 
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_81604381047 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_81604381051 object-group 
CSM_INLINE_src_rule_81604381051 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP’s and Controllers in stores
 permit object-group CSM_INLINE_svc_rule_81604381043 object-group 
CSM_INLINE_src_rule_81604381043 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group STORE-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large store Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
```

```
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
```

```
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication RETAIL
 no exec
 transport preferred none
 transport output none
line 67
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
 stopbits 1
line 131
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
scheduler allocate 20000 1000
scheduler interval 500
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

r-a2-mini-1

```
!
! Last configuration change at 00:50:32 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 00:50:35 PST Sat Apr 30 2011 by retail
!
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname R-A2-Mini-1
!
boot-start-marker
boot system flash0 c1900-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
```

```
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PST recurring
service-module wlan-ap 0 bootimage autonomous
!
no ipv6 cef
no ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip port-map user-8443 port tcp 8443
ip inspect log drop-pkt
ip inspect audit-trail
ip ips config location flash0: retries 1 timeout 1
ip ips notify SDEE
ip ips name Store-IPS
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
!
parameter-map type inspect Inspect-1
 audit-trail on
parameter-map type inspect global
 WAAS enable

parameter-map type trend-global trend-glob-map
password encryption aes
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1721465088
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1721465088
 revocation-check none
 rsakeypair TP-self-signed-1721465088
!
!
crypto pki certificate chain TP-self-signed-1721465088
 certificate self-signed 01
  <removed>
    quit
license udi pid CISCO1941W-A/K9 sn <removed>
hw-module ism 0
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Stores-ALL
 description all store networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_68719541425
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for stores
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_68719541431
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
```

```
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_68719541435
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_68719541457
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_68719541461
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_68719541465
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_73014451187
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_73014451193
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_73014451223
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_68719541409
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network CSM_INLINE_src_rule_68719541427
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_src_rule_68719541429
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_68719541433
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_68719541437
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_73014451215
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
```

```
object-group network CSM_INLINE_src_rule_73014451217
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group service CSM_INLINE_svc_rule_68719541409
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_68719541425
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_68719541427
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_68719541429
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_68719541431
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
```

```
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_68719541437
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_68719541439
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_68719541455
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_68719541457
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
```

```
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_68719541459
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group service CSM_INLINE_svc_rule_73014451187
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_73014451193
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_73014451195
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_73014451197
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
```

```
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_73014451203
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_73014451205
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_73014451207
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_73014451209
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_73014451211
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_73014451213
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
```

```
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_73014451215
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_73014451217
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_73014451221
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_73014451223
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_73014451388
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_73014451393
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_73014451395
```

```
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451397
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451404
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451406
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group network DC-Applications
 description Applications in the Data Center that are non-PCI related(Optimized by
CS-Manager)
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network STORE-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
```

```
!
redundancy
!
!
!
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
```

```
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url "*SalesReport*"
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map type inspect CSM_ZBF_POLICY_S_Security_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Data_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Data-W_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAN_S_Guest
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAN_S_Data-W
```

```
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Voice_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Guest_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_MGMT_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_LOOPBACK_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_POS-W
 class class-default
  drop log
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_Partners
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_POS
 class class-default
  drop log
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_28
```

```
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_S_MGMT_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Voice_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Guest_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
```

```
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_S_Partners_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Security_S_POS
 class class-default
  drop log
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
policy-map type inspect CSM_ZBF_POLICY_S_Data_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Data-W_S_POS-W
 class class-default
  drop log
!
zone security S_WAN
 description Store WAN Link
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_S_WAN_S_Data-W
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_S_WAN_S_Guest
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_LOOPBACK_S_POS-W
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_MGMT_S_POS
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_MGMT_S_POS-W
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Security_S_POS
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Security_S_POS-W
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_POS
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_POS-W
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_Partners
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS-W
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Data_S_POS
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Data_S_POS-W
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Data-W_S_POS
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
```

```
 service-policy type inspect CSM_ZBF_POLICY_S_Data-W_S_POS-W
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Guest_S_POS
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Guest_S_POS-W
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Partners_S_POS
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Voice_S_POS
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Voice_S_POS-W
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.158.1 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface GigabitEthernet0/0
 ip address 10.10.255.144 255.255.255.0
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface wlan-ap0
 description Service module interface to manage the embedded AP
 ip address 10.10.158.33 255.255.255.252
 zone-member security S_WLC-AP
 service-module ip address 10.10.158.34 255.255.255.252
 service-module ip default-gateway 10.10.158.33
 arp timeout 0
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/1
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.144.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
 standby 11 ip 10.10.144.1
 standby 11 priority 101
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.145.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.145.1
 standby 12 priority 101
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.146.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.146.1
 standby 13 priority 101
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.14
 description WIRELESS
 encapsulation dot1Q 14
 ip address 10.10.147.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.147.1
 standby 14 priority 101
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.148.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS-W
 standby 15 ip 10.10.148.1
 standby 15 priority 101
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.149.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.149.1
 standby 16 priority 101
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.17
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.150.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.150.1
 standby 17 priority 101
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.151.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.151.1
 standby 18 priority 101
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.19
 description WAAS
 encapsulation dot1Q 19
 ip address 10.10.152.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.152.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.20
 zone-member security S_Security
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.159.2 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.159.1
 standby 100 priority 101
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Wlan-GigabitEthernet0/0
 description Internal switch interface connecting to the embedded AP
 zone-member security S_WLC-AP
 service-module ip address 10.10.158.34 255.255.255.252
 service-module ip default-gateway 10.10.158.33
!
interface Vlan1
 no ip address
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
!
interface Vlan15
 no ip address
 zone-member security S_POS-W
!
interface Vlan1000
 no ip address
 zone-member security S_MGMT
!
router ospf 5
 router-id 10.10.158.1
 passive-interface default
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.10.255.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_68719541409 object-group
CSM_INLINE_src_rule_68719541409 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451205 object-group DC-POS-Oracle
object-group STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451209 object-group DC-POS-SAP object-group
STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451213 object-group DC-POS-Tomax
object-group STORE-POS
```

```
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451215 object-group 
CSM_INLINE_src_rule_73014451215 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_68719541455 object-group DC-Voice object-group 
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_73014451187 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_73014451187
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_73014451193 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_73014451193
ip access-list extended CSM_ZBF_CMAP_ACL_15
 remark Store to Data Center for NTP
 permit object-group NTP object-group Stores-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_73014451221 object-group Stores-ALL object-group 
ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541425 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_68719541425
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store UCS Express to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_73014451197 object-group Stores-ALL object-group 
vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_73014451223 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_73014451223
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Stores-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Store to Data Center Physical Security
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_68719541435
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_68719541439 object-group Stores-ALL object-group 
DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_73014451388 object-group Stores-ALL object-group 
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_68719541431 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_68719541431
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451203 object-group STORE-POS object-group 
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451207 object-group STORE-POS object-group 
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451211 object-group STORE-POS object-group 
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_25
```

```
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451217 object-group 
CSM_INLINE_src_rule_73014451217 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451393 object-group STORE-POS object-group 
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451395 object-group STORE-POS object-group 
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Permit POS clients to talk to store POS server
 permit object-group CSM_INLINE_svc_rule_73014451397 object-group STORE-POS object-group 
STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451404 object-group Stores-ALL object-group 
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541427 object-group 
CSM_INLINE_src_rule_68719541427 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451406 object-group Stores-ALL object-group 
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_68719541459 object-group Stores-ALL object-group 
DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_68719541465
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_68719541461
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_68719541457 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_68719541457
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS Express
 permit object-group CSM_INLINE_svc_rule_73014451195 object-group vSphere-1 object-group 
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_68719541433 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_68719541437 object-group 
CSM_INLINE_src_rule_68719541437 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP’s and Controllers in stores
 permit object-group CSM_INLINE_svc_rule_68719541429 object-group
CSM_INLINE_src_rule_68719541429 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group STORE-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large store Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group causer v3 priv
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
!
banner exec C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITACCESS IS A
VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication RETAIL
 no exec
 transport preferred none
 transport output none
line 67
 no activation-character
 no exec
 transport preferred none
 transport output none
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

R-a2-Small

```
!
! Last configuration change at 00:44:15 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 00:44:16 PSTDST Sat Apr 30 2011 by retail
!
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname R-A2-Small-1
!
boot-start-marker
boot system flash0 c2900-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
```

```
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PSTDST recurring
!
no ipv6 cef
ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip port-map user-8443 port tcp 8443
ip ips notify SDEE
ip ips name Retail-PCI
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
!
parameter-map type inspect global
 WAAS enable
parameter-map type inspect Inspect-1
 audit-trail on

parameter-map type trend-global trend-glob-map
!
!
!
!
```

```
password encryption aes
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-503450500
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-503450500
 revocation-check none
 rsakeypair TP-self-signed-503450500
!
!
crypto pki certificate chain TP-self-signed-503450500
 certificate self-signed 01
  <removed>
    quit
voice-card 0
!
!
!
!
!
!
!
license udi pid CISCO2921/K9 sn <removed>
hw-module ism 0
!
hw-module sm 1
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Stores-ALL
 description all store networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_68719541425
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
```

```
 description Central Wireless Controllers for stores
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_68719541431
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_68719541435
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_68719541457
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_68719541461
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_dst_rule_68719541465
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_73014451187
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
```

```
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_73014451193
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_73014451223
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_68719541409
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network CSM_INLINE_src_rule_68719541427
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
object-group network CSM_INLINE_src_rule_68719541429
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_68719541433
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_68719541437
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
```

```
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_73014451215
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_73014451217
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group service CSM_INLINE_svc_rule_68719541409
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_68719541425
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_68719541427
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_68719541429
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_68719541431
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_68719541437
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_68719541439
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_68719541455
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_68719541457
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service Netbios
```

```
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_68719541459
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group service CSM_INLINE_svc_rule_73014451187
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_73014451193
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_73014451195
 description Generated by CS-Manager from service of ZbfInspectRule# 0 
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
```

```
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_73014451197
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_73014451203
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_73014451205
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_73014451207
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_73014451209
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
```

```
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_73014451211
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_73014451213
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_73014451215
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_73014451217
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_73014451221
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_73014451223
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_73014451388
```

```
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_73014451393
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_73014451395
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451397
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451404
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451406
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group network DC-Applications
 description Applications in the Data Center that are non-PCI related(Optimized by
CS-Manager)
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
```

```
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network POS-Store-SMALL-1
 description Small Store POS devices
 host 10.10.128.81
 host 10.10.128.82
!
object-group network STORE-POS
 group-object POS-Store-SMALL-1
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed> username bmcgloth privilege 15 secret 5
<removed>
username csmadmin privilege 15 secret 5 <removed>
!
redundancy
!
!
!
!
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
```

```
 match access-group name CSM_ZBF_CMAP_ACL_25
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url “*SalesReport*”
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
```

```
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
```

```
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
!
zone security S_WAN
 description Store WAN Link
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
```

```
 description VLAN15 Store Wireless POS
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.142.1 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface GigabitEthernet0/0
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.128.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_POS
 standby 11 ip 10.10.128.1
 standby 11 priority 101
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
```

```
!
interface GigabitEthernet0/0.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.129.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.129.1
 standby 12 priority 101
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.130.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.130.1
 standby 13 priority 101
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.14
 description WIRELESS
 encapsulation dot1Q 14
 ip address 10.10.131.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.131.1
 standby 14 priority 101
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.132.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_POS-W
 standby 15 ip 10.10.132.1
 standby 15 priority 101
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.133.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.133.1
 standby 16 priority 101
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.17
```

```
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.134.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.134.1
 standby 17 priority 101
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.135.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.135.1
 standby 18 priority 101
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.19
 description WAAS
 encapsulation dot1Q 19
 ip address 10.10.136.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.136.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.20
 description SECURITY-SYSTEMS
 encapsulation dot1Q 20
 ip address 10.10.137.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Security
 standby 20 ip 10.10.137.1
 standby 20 priority 101
 standby 20 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.143.2 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.143.1
 standby 100 priority 101
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface ISM0/0
 no ip address
 shutdown
 !Application: Online on SME
 hold-queue 60 out
!
```

```
interface GigabitEthernet0/1
 ip address 10.10.255.128 255.255.255.0
 ip ips Retail-PCI in
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface GigabitEthernet0/2
 ip address 10.10.254.128 255.255.255.0
 ip ips Retail-PCI in
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface ISM0/1
 description Internal switch interface connected to Internal Service Module
 shutdown
!
interface SM1/0
 no ip address
 zone-member security S_Security
 shutdown
 service-module fail-open
 hold-queue 60 out
!
interface SM1/1
 description Internal switch interface connected to Service Module
!
interface Vlan1
 no ip address
 zone-member security S_POS
!
!
router ospf 5
 router-id 10.10.142.1
 passive-interface default
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.10.255.11
ip route 0.0.0.0 0.0.0.0 10.10.254.11 50
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_68719541409 object-group 
CSM_INLINE_src_rule_68719541409 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451205 object-group DC-POS-Oracle 
object-group STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451209 object-group DC-POS-SAP object-group 
STORE-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451213 object-group DC-POS-Tomax 
object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451215 object-group 
CSM_INLINE_src_rule_73014451215 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_68719541455 object-group DC-Voice object-group 
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_73014451187 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_73014451187
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_73014451193 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_73014451193
ip access-list extended CSM_ZBF_CMAP_ACL_15
 remark Store to Data Center for NTP
 permit object-group NTP object-group Stores-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_73014451221 object-group Stores-ALL object-group 
ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541425 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_68719541425
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store UCS Express to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_73014451197 object-group Stores-ALL object-group 
vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_73014451223 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_73014451223
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Stores-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Store to Data Center Physical Security
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_68719541435
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_68719541439 object-group Stores-ALL object-group 
DC-WAAS
```

```
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_73014451388 object-group Stores-ALL object-group 
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_68719541431 object-group Stores-ALL object-group 
CSM_INLINE_dst_rule_68719541431
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451203 object-group STORE-POS object-group 
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451207 object-group STORE-POS object-group 
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451211 object-group STORE-POS object-group 
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451217 object-group 
CSM_INLINE_src_rule_73014451217 object-group STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451393 object-group STORE-POS object-group 
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451395 object-group STORE-POS object-group 
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Permit POS clients to talk to store POS server
 permit object-group CSM_INLINE_svc_rule_73014451397 object-group STORE-POS object-group 
STORE-POS
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451404 object-group Stores-ALL object-group 
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541427 object-group 
CSM_INLINE_src_rule_68719541427 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451406 object-group Stores-ALL object-group 
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_68719541459 object-group Stores-ALL object-group 
DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_68719541465
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Stores-ALL object-group CSM_INLINE_dst_rule_68719541461
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Stores-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_68719541457 object-group Stores-ALL object-group
CSM_INLINE_dst_rule_68719541457
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS Express
 permit object-group CSM_INLINE_svc_rule_73014451195 object-group vSphere-1 object-group
Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_68719541433 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_68719541437 object-group
CSM_INLINE_src_rule_68719541437 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP’s and Controllers in stores
 permit object-group CSM_INLINE_svc_rule_68719541429 object-group
CSM_INLINE_src_rule_68719541429 object-group Stores-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group STORE-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large store Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
```

```
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
banner exec C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
```

```
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 no exec
 transport preferred none
 transport output none
line 67
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
 stopbits 1
 flowcontrol software
line 131
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
 stopbits 1
 flowcontrol software
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

RAGG-1-running

```
!Command: show running-config
!Time: Sun Apr 24 16:49:11 2011

version 5.1(2)
hostname RAGG-1
vdc RAGG-1 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 32 maximum 32
  limit-resource u6route-mem minimum 16 maximum 16
  limit-resource m4route-mem minimum 48 maximum 48
  limit-resource m6route-mem minimum 8 maximum 8
vdc vdc1 id 2
  allocate interface Ethernet1/1,Ethernet1/3,Ethernet1/5,Ethernet1/7,Ethernet1/25-32
  allocate interface Ethernet2/1-12
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
vdc vdc2 id 3
  allocate interface Ethernet1/2,Ethernet1/4,Ethernet1/6,Ethernet1/8-24
  allocate interface Ethernet2/13-48
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5

feature privilege
feature tacacs+
username admin password 5 <removed>   role network-admin
username retail password 5 <removed> role network-admin
username bart password 5 <removed> role network-admin
username emc-ncm password 5 <removed>  role network-admin
enable secret 5 <removed>

banner motd @
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
@

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host RAGG-1 192.168.42.36
tacacs-server key 7 “<removed>”
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.42.36/32
  20 permit ip 192.168.41.101/32 192.168.42.36/32
  30 permit ip 192.168.41.102/32 192.168.42.36/32
  40 permit ip 192.168.42.111/32 192.168.42.36/32
  50 permit ip 192.168.42.122/32 192.168.42.36/32
  60 permit ip 192.168.42.131/32 192.168.42.36/32
  70 permit ip 192.168.42.133/32 192.168.42.36/32
  80 permit ip 192.168.42.138/32 192.168.42.36/32
  90 permit ip 10.19.151.99/32 192.168.42.36/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.42.36/32
  20 deny ip any any
ip access-list copp-system-acl-bgp
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ipv6 access-list copp-system-acl-bgp6
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ip access-list copp-system-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
ip access-list copp-system-acl-glbp
  10 permit udp any eq 3222 224.0.0.0/24 eq 3222
```

```
ip access-list copp-system-acl-hsrp
  10 permit udp any 224.0.0.0/24 eq 1985
ip access-list copp-system-acl-icmp
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-acl-icmp6
  10 permit icmp any any echo-request
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-acl-icmp6-msgs
  10 permit icmp any any router-advertisement
  20 permit icmp any any router-solicitation
  30 permit icmp any any nd-na
  40 permit icmp any any nd-ns
  50 permit icmp any any mld-query
  60 permit icmp any any mld-report
  70 permit icmp any any mld-reduction
ip access-list copp-system-acl-igmp
  10 permit igmp any 224.0.0.0/3
ip access-list copp-system-acl-msdp
  10 permit tcp any gt 1024 any eq 639
  20 permit tcp any eq 639 any gt 1024
ip access-list copp-system-acl-ntp
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ipv6 access-list copp-system-acl-ntp6
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ip access-list copp-system-acl-ospf
  10 permit ospf any any
ipv6 access-list copp-system-acl-ospf6
  10 permit 89 any any
ip access-list copp-system-acl-pim
  10 permit pim any 224.0.0.0/24
  20 permit udp any any eq pim-auto-rp
ip access-list copp-system-acl-pim-reg
  10 permit pim any any
ipv6 access-list copp-system-acl-pim6
  10 permit 103 any ff02::d/128
  20 permit udp any any eq pim-auto-rp
ip access-list copp-system-acl-radius
  10 permit udp any any eq 1812
  20 permit udp any any eq 1813
  30 permit udp any any eq 1645
  40 permit udp any any eq 1646
  50 permit udp any eq 1812 any
  60 permit udp any eq 1813 any
  70 permit udp any eq 1645 any
  80 permit udp any eq 1646 any
ipv6 access-list copp-system-acl-radius6
  10 permit udp any any eq 1812
  20 permit udp any any eq 1813
  30 permit udp any any eq 1645
  40 permit udp any any eq 1646
  50 permit udp any eq 1812 any
  60 permit udp any eq 1813 any
  70 permit udp any eq 1645 any
  80 permit udp any eq 1646 any
ip access-list copp-system-acl-rip
  10 permit udp any 224.0.0.0/24 eq rip
ip access-list copp-system-acl-sftp
  10 permit tcp any any eq 115
  20 permit tcp any eq 115 any
ip access-list copp-system-acl-snmp
  10 permit udp any any eq snmp
  20 permit udp any any eq snmptrap
ip access-list copp-system-acl-ssh
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
ipv6 access-list copp-system-acl-ssh6
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
ip access-list copp-system-acl-tacacs
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
ipv6 access-list copp-system-acl-tacacs6
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
ip access-list copp-system-acl-telnet
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
ipv6 access-list copp-system-acl-telnet6
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
ip access-list copp-system-acl-tftp
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
ipv6 access-list copp-system-acl-tftp6
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
ip access-list copp-system-acl-traceroute
  10 permit icmp any any ttl-exceeded
  20 permit icmp any any port-unreachable
ip access-list copp-system-acl-undesirable
  10 permit udp any any eq 1434
ip access-list copp-system-acl-vpc
  10 permit udp any any eq 3200
ip access-list copp-system-acl-vrrp
  10 permit 112 any 224.0.0.0/24
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-bgp
  match access-group name copp-system-acl-bgp6
  match access-group name copp-system-acl-eigrp
  match access-group name copp-system-acl-igmp
  match access-group name copp-system-acl-msdp
  match access-group name copp-system-acl-ospf
  match access-group name copp-system-acl-ospf6
  match access-group name copp-system-acl-pim
  match access-group name copp-system-acl-pim6
  match access-group name copp-system-acl-rip
  match access-group name copp-system-acl-vpc
class-map type control-plane match-any copp-system-class-exception
  match exception ip option
  match exception ip icmp unreachable
  match exception ipv6 option
  match exception ipv6 icmp unreachable
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-glbp
  match access-group name copp-system-acl-hsrp
  match access-group name copp-system-acl-vrrp
  match access-group name copp-system-acl-icmp6-msgs
  match access-group name copp-system-acl-pim-reg
class-map type control-plane match-any copp-system-class-management
  match access-group name copp-system-acl-ftp
  match access-group name copp-system-acl-ntp
  match access-group name copp-system-acl-ntp6
  match access-group name copp-system-acl-radius
  match access-group name copp-system-acl-sftp
  match access-group name copp-system-acl-snmp
  match access-group name copp-system-acl-ssh
  match access-group name copp-system-acl-ssh6
  match access-group name copp-system-acl-tacacs
  match access-group name copp-system-acl-telnet
  match access-group name copp-system-acl-tftp
  match access-group name copp-system-acl-tftp6
  match access-group name copp-system-acl-radius6
  match access-group name copp-system-acl-tacacs6
  match access-group name copp-system-acl-telnet6
class-map type control-plane match-any copp-system-class-monitoring
  match access-group name copp-system-acl-icmp
  match access-group name copp-system-acl-icmp6
  match access-group name copp-system-acl-traceroute
class-map type control-plane match-any copp-system-class-normal
  match protocol arp
class-map type control-plane match-any copp-system-class-redirect
  match redirect dhcp-snoop
  match redirect arp-inspect
class-map type control-plane match-any copp-system-class-undesirable
  match access-group name copp-system-acl-undesirable
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 39600 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-important
    police cir 1060 kbps bc 1000 ms conform transmit violate drop
  class copp-system-class-management
    police cir 10000 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-normal
    police cir 680 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-redirect
    police cir 280 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-monitoring
    police cir 130 kbps bc 1000 ms conform transmit violate drop
  class copp-system-class-exception
    police cir 360 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-undesirable
    police cir 32 kbps bc 250 ms conform drop violate drop
  class class-default
    police cir 100 kbps bc 250 ms conform transmit violate drop
control-plane
  service-policy input copp-system-policy
snmp-server user bart network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user admin network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user retail network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user emc-ncm network-admin auth md5 <removed> priv <removed> localizedkey
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
  ip route 0.0.0.0/0 192.168.42.1
vlan 1
```

```
interface mgmt0
  ip address 192.168.42.36/24
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
  logout-warning 20
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
boot kickstart bootflash:/n7000-s1-kickstart.5.1.2.bin sup-1
boot system bootflash:/n7000-s1-dk9.5.1.2.bin sup-1
boot kickstart bootflash:/n7000-s1-kickstart.5.1.2.bin sup-2
boot system bootflash:/n7000-s1-dk9.5.1.2.bin sup-2
logging server 192.168.42.124 6 use-vrf management
```

RAGG-1-vdc1-running

```
!Command: show running-config
!Time: Sun Apr 24 16:50:08 2011

version 5.1(2)
hostname vdc1

feature privilege
feature tacacs+
cfs eth distribute
feature ospf
feature pim
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature glbp
feature vpc

username admin password 5 <removed> role vdc-admin
username retail password 5 <removed> role vdc-admin
username emc-ncm password 5 <removed> role vdc-admin
username bart password 5 <removed>  role vdc-admin
enable secret 5 <removed>

banner motd @
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
@
```

```
ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    source-interface loopback0
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.1.11/32
  20 permit ip 192.168.41.101/32 192.168.1.11/32
  30 permit ip 192.168.41.102/32 192.168.1.11/32
  40 permit ip 192.168.42.111/32 192.168.1.11/32
  50 permit ip 192.168.42.122/32 192.168.1.11/32
  60 permit ip 192.168.42.131/32 192.168.1.11/32
  70 permit ip 192.168.42.133/32 192.168.1.11/32
  80 permit ip 192.168.42.138/32 192.168.1.11/32
  90 permit ip 10.19.151.99/32 192.168.1.11/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.1.11/32
  20 deny ip any any
snmp-server source-interface trap loopback0
snmp-server source-interface inform loopback0
snmp-server user bart vdc-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user admin vdc-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user retail vdc-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user emc-ncm vdc-admin auth md5 <removed> priv <removed> localizedkey
no snmp-server enable traps entity entity_mib_change
no snmp-server enable traps entity entity_module_status_change
no snmp-server enable traps entity entity_power_status_change
no snmp-server enable traps entity entity_module_inserted
no snmp-server enable traps entity entity_module_removed
no snmp-server enable traps entity entity_unrecognised_module
no snmp-server enable traps entity entity_fan_status_change
no snmp-server enable traps entity entity_power_out_change
no snmp-server enable traps link linkDown
no snmp-server enable traps link linkUp
no snmp-server enable traps link IETF-extended-linkDown
no snmp-server enable traps link IETF-extended-linkUp
no snmp-server enable traps link cisco-extended-linkDown
no snmp-server enable traps link cisco-extended-linkUp
snmp-server enable traps callhome event-notify
snmp-server enable traps callhome smtp-send-fail
snmp-server enable traps cfs state-change-notif
snmp-server enable traps cfs merge-failure
no snmp-server enable traps rf redundancy_framework
snmp-server enable traps aaa server-state-change
no snmp-server enable traps license notify-license-expiry
no snmp-server enable traps license notify-no-license-for-feature
no snmp-server enable traps license notify-licensefile-missing
no snmp-server enable traps license notify-license-expiry-warning
snmp-server enable traps hsrp state-change
no snmp-server enable traps upgrade UpgradeOpNotifyOnCompletion
no snmp-server enable traps upgrade UpgradeJobStatusNotify
snmp-server enable traps feature-control FeatureOpStatusChange
snmp-server enable traps link cisco-xcvr-mon-status-chg
snmp-server enable traps vtp notifs
snmp-server enable traps vtp vlancreate
```

```
snmp-server enable traps vtp vlandelete
snmp-server enable traps bridge newroot
snmp-server enable traps bridge topologychange
snmp-server enable traps stpx inconsistency
snmp-server enable traps stpx root-inconsistency
snmp-server enable traps stpx loop-inconsistency
aaa authentication login default group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
vlan 1,3,151,161

interface Vlan1

interface Vlan3
  no shutdown
  ip address 192.168.10.61/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 3
  ip ospf hello-interval 1
  ip router ospf 5 area 0.0.0.0

interface Vlan151
  no shutdown
  ip address 192.168.152.3/24
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf priority 3
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 10 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.152.1

interface Vlan161
  no shutdown
  ip address 192.168.162.3/24
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf priority 5
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 10 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.162.1

interface port-channel99
  switchport
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/1
  description 10Gig LINK to RCORE-1 T2/1
  no switchport
  logging event port link-status
  no ip redirects
  ip address 192.168.10.14/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 6
  ip ospf hello-interval 2
  ip ospf network point-to-point
  ip router ospf 5 area 0.0.0.0
  ip pim sparse-mode
  ip igmp version 3
  no shutdown

interface Ethernet1/3
  description 10Gig LINK to RCORE-2 T2/1
  no switchport
  logging event port link-status
  no ip redirects
  ip address 192.168.10.22/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 6
  ip ospf hello-interval 2
  ip ospf network point-to-point
  ip router ospf 5 area 0.0.0.0
  ip pim sparse-mode
  ip igmp version 3
  no shutdown

interface Ethernet1/5
  description to DC-ASA-1 vc1 T0/6
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 161
  spanning-tree port type normal
  no shutdown

interface Ethernet1/7
  description to DC-ASA-1 vc2 T0/8
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 151
  spanning-tree port type normal
  no shutdown

interface Ethernet1/25
  no switchport

interface Ethernet1/26
  no switchport

interface Ethernet1/27
  no switchport

interface Ethernet1/28
  no switchport

interface Ethernet1/29
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown
```

```
interface Ethernet1/30
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet1/31
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet1/32
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet2/1
  no switchport

interface Ethernet2/2
  no switchport

interface Ethernet2/3
  no switchport

interface Ethernet2/4
  no switchport

interface Ethernet2/5
  no switchport

interface Ethernet2/6
  no switchport

interface Ethernet2/7
  no switchport

interface Ethernet2/8
  no switchport

interface Ethernet2/9
  no switchport

interface Ethernet2/10
  no switchport

interface Ethernet2/11
  no switchport

interface Ethernet2/12
  no switchport

interface loopback0
  ip address 192.168.1.11/32
  ip router ospf 5 area 0.0.0.0
logging server 192.168.42.124 6
logging source-interface loopback 0
  logout-warning 20
```

```
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
router ospf 5
  router-id 192.168.1.11
  area 0.0.0.81 nssa
  area 0.0.0.0 range 192.168.1.11/32
  area 0.0.0.0 range 192.168.10.12/30
  area 0.0.0.0 range 192.168.10.20/30
  area 0.0.0.0 range 192.168.10.60/30
  area 0.0.0.81 range 192.168.152.0/24
  area 0.0.0.81 range 192.168.162.0/24
  area 0.0.0.0 authentication message-digest
  area 0.0.0.81 authentication message-digest
  timers throttle spf 10 100 5000
  auto-cost reference-bandwidth 10000
ip pim ssm range 232.0.0.0/8
```

RAGG-1-vdc2-running

```
!Command: show running-config
!Time: Sun Apr 24 16:50:48 2011

version 5.1(2)
hostname vdc2

feature privilege
feature tacacs+
cfs eth distribute
feature ospf
feature pim
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature vpc

username admin password 5 <removed>   role vdc-admin
username retail password 5 <removed>   role vdc-admin
username bart password 5 <removed>   role vdc-admin
username emc-ncm password 5 <removed> role vdc-admin
enable secret 5 <removed>

banner motd @
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
```

```
@

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
tacacs-server key 7 “<removed>”
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf servers1
    source-interface loopback0
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.1.31/32
  20 permit ip 192.168.41.101/32 192.168.1.31/32
  30 permit ip 192.168.41.102/32 192.168.1.31/32
  40 permit ip 192.168.42.111/32 192.168.1.31/32
  50 permit ip 192.168.42.122/32 192.168.1.31/32
  60 permit ip 192.168.42.131/32 192.168.1.31/32
  70 permit ip 192.168.42.133/32 192.168.1.31/32
  80 permit ip 192.168.42.138/32 192.168.1.31/32
  90 permit ip 10.19.151.99/32 192.168.1.31/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.1.31/32
  20 deny ip any any
snmp-server source-interface trap loopback0
snmp-server source-interface inform loopback0
snmp-server user bart vdc-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user admin vdc-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user retail vdc-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user emc-ncm vdc-admin auth md5 <removed> priv <removed> localizedkey
no snmp-server enable traps entity entity_mib_change
no snmp-server enable traps entity entity_module_status_change
no snmp-server enable traps entity entity_power_status_change
no snmp-server enable traps entity entity_module_inserted
no snmp-server enable traps entity entity_module_removed
no snmp-server enable traps entity entity_unrecognised_module
no snmp-server enable traps entity entity_fan_status_change
no snmp-server enable traps entity entity_power_out_change
no snmp-server enable traps link linkDown
no snmp-server enable traps link linkUp
no snmp-server enable traps link IETF-extended-linkDown
no snmp-server enable traps link IETF-extended-linkUp
no snmp-server enable traps link cisco-extended-linkDown
no snmp-server enable traps link cisco-extended-linkUp
snmp-server enable traps callhome event-notify
snmp-server enable traps callhome smtp-send-fail
snmp-server enable traps cfs state-change-notif
snmp-server enable traps cfs merge-failure
no snmp-server enable traps rf redundancy_framework
snmp-server enable traps aaa server-state-change
no snmp-server enable traps license notify-license-expiry
no snmp-server enable traps license notify-no-license-for-feature
no snmp-server enable traps license notify-licensefile-missing
no snmp-server enable traps license notify-license-expiry-warning
snmp-server enable traps hsrp state-change
no snmp-server enable traps upgrade UpgradeOpNotifyOnCompletion
no snmp-server enable traps upgrade UpgradeJobStatusNotify
snmp-server enable traps feature-control FeatureOpStatusChange
snmp-server enable traps link cisco-xcvr-mon-status-chg
snmp-server enable traps vtp notifs
```

```
snmp-server enable traps vtp vlancreate
snmp-server enable traps vtp vlandelete
snmp-server enable traps bridge newroot
snmp-server enable traps bridge topologychange
snmp-server enable traps stpx inconsistency
snmp-server enable traps stpx root-inconsistency
snmp-server enable traps stpx loop-inconsistency
aaa authentication login default group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context VPC
vrf context servers1
  ip route 0.0.0.0/0 192.168.162.1
  ip route 192.168.41.0/24 192.168.42.135
  ip pim ssm range 232.0.0.0/8
vrf context servers2
  ip pim ssm range 232.0.0.0/8
vrf context management
vlan 1
vlan 36
  name DeviceMgmtHigh
vlan 37
  name DeviceMgmtLow
vlan 38
  name UIM-OS-INSTALL
vlan 40-41
vlan 42
  name CoreManagement
vlan 43
  name WirelessSystems
vlan 44
  name PhysicalSec
vlan 45
  name VOICE
vlan 52
  name POS
vlan 151-152,154,161-162,164,180-181
spanning-tree domain 777
spanning-tree vlan 1 priority 4096
ip prefix-list VLAN41 seq 5 permit 192.168.41.0/24
route-map VLAN41 permit 20
  match ip address prefix-list VLAN41
vpc domain 99
  peer-switch
  peer-keepalive destination 192.168.10.66 source 192.168.10.65 vrf VPC
  peer-gateway


interface Vlan1
  no shutdown
  no ip redirects

interface Vlan36
  no shutdown
  description DeviceMgmtHigh
  vrf member servers1
  no ip redirects
  ip address 192.168.36.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
```

```
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 110 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.36.1

  interface Vlan37
    no shutdown
    description DeviceMgmtLow
    vrf member servers1
    no ip redirects
    ip address 192.168.37.3/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 110 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.37.1

  interface Vlan38
    no shutdown
    description UIM OS Install only
    vrf member servers1
    no ip redirects
    ip address 192.168.38.201/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3

  interface Vlan40
    no shutdown
    vrf member servers1
    no ip redirects
    ip address 192.168.40.3/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 120 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.40.1

  interface Vlan41
    shutdown
    description SHUTDOWN - NOW ROUTE VIA HyTrust
    vrf member servers1
    no ip redirects
    ip address 192.168.41.3/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 120 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.41.1

  interface Vlan42
    no shutdown
    vrf member servers1
    no ip redirects
    ip address 192.168.42.3/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 120 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.42.1

  interface Vlan43
    no shutdown
    description Wireless Systems
    vrf member servers1
    no ip redirects
    ip address 192.168.43.3/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 110 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.43.1

  interface Vlan44
    no shutdown
    description Wireless Systems
    vrf member servers1
    no ip redirects
    ip address 192.168.44.3/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 110 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.44.1

  interface Vlan45
    no shutdown
    description VOICE
    vrf member servers1
    no ip redirects
    ip address 192.168.45.3/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 110 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.45.1

  interface Vlan52
    no shutdown
    description POS
    vrf member servers1
    no ip redirects
    ip address 192.168.52.3/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 110 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.52.1

  interface Vlan154
    no shutdown
    vrf member servers2
    no ip redirects
    ip address 192.168.152.5/24
    ip ospf authentication message-digest
    ip ospf message-digest-key 1 md5 3 <removed>
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 110 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.152.7

  interface Vlan164
    no shutdown
    vrf member servers1
    no ip redirects
    ip address 192.168.162.5/24
    ip ospf authentication message-digest
    ip ospf message-digest-key 1 md5 3 <removed>
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 120 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.162.7

  interface Vlan180
    no shutdown
    vrf member servers1
    no ip redirects
    ip address 192.168.180.3/24
    ip ospf passive-interface
```

```
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 1
      authentication text c1sc0
      preempt delay minimum 180
      priority 120 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.180.1

  interface Vlan181
    no shutdown
    vrf member servers2
    no ip redirects
    ip address 192.168.181.3/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 1
      authentication text c1sc0
      preempt delay minimum 180
      priority 110 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.181.1

  interface port-channel1
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 38,41-42,44
    vpc 1

  interface port-channel2
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 38,41-42,44
    vpc 2

  interface port-channel3
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 38,41-45,52
    vpc 3

  interface port-channel4
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 38,41-45,52
    vpc 4

  interface port-channel11
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 38,41,45-46
    spanning-tree port type edge trunk
    vpc 11

  interface port-channel12
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 38,41,45-46
    spanning-tree port type edge trunk
    vpc 12
```

```
interface port-channel99
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  spanning-tree port type network
  spanning-tree guard loop
  vpc peer-link

interface Ethernet1/2
  description F-UCS-1_E2/1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 11 mode active
  no shutdown

interface Ethernet1/4
  description F-UCS-1_E2/2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 11 mode active
  no shutdown

interface Ethernet1/6
  description F-UCS-2_E2/1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 12 mode active
  no shutdown

interface Ethernet1/8
  description F-UCS-2_E2/2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 12 mode active
  no shutdown

interface Ethernet1/9
  description SACCESS-3 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 3 mode active
  no shutdown

interface Ethernet1/10
  description SACCESS-3 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 3 mode active
  no shutdown

interface Ethernet1/11
  description SACCESS-4 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 4 mode active
  no shutdown
```

```
interface Ethernet1/12
  description SACCESS-4 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 4 mode active
  no shutdown

interface Ethernet1/13
  description SACCESS-1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  channel-group 1 mode active
  no shutdown

interface Ethernet1/14
  description SACCESS-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  channel-group 2 mode active
  no shutdown

interface Ethernet1/15
  description to RSERV-1 T2/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 162
  spanning-tree port type normal
  no shutdown

interface Ethernet1/16
  description to RSERV-1 T2/2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 152
  spanning-tree port type normal
  no shutdown

interface Ethernet1/17
  description to RSERV-1 T2/5
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 41-44,164
  spanning-tree port type normal
  no shutdown

interface Ethernet1/18
  description to RSERV-1 T2/6
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 154
  spanning-tree port type normal
  no shutdown

interface Ethernet1/19
  description to DC-ASA-1 vc1 T5/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 162
  spanning-tree port type normal
  no shutdown
```

```
interface Ethernet1/20
  description to DC-ASA-1 vc2 T7/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 152
  spanning-tree port type normal
  no shutdown

interface Ethernet1/21
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/22
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/23
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/24
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet2/13
  description SACCESS-5
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  no shutdown

interface Ethernet2/14
  description linkstate for vpc
  no switchport
  vrf member VPC
  ip address 192.168.10.65/30
  no shutdown

interface Ethernet2/15
  no switchport

interface Ethernet2/16
  no switchport
```

```
interface Ethernet2/17
  no switchport

interface Ethernet2/18
  no switchport

interface Ethernet2/19
  no switchport

interface Ethernet2/20
  no switchport

interface Ethernet2/21
  no switchport

interface Ethernet2/22
  no switchport

interface Ethernet2/23
  no switchport

interface Ethernet2/24
  no switchport

interface Ethernet2/25
  no switchport

interface Ethernet2/26
  no switchport

interface Ethernet2/27
  no switchport

interface Ethernet2/28
  no switchport

interface Ethernet2/29
  no switchport

interface Ethernet2/30
  no switchport

interface Ethernet2/31
  no switchport

interface Ethernet2/32
  no switchport

interface Ethernet2/33
  no switchport

interface Ethernet2/34
  no switchport

interface Ethernet2/35
  no switchport

interface Ethernet2/36
  no switchport

interface Ethernet2/37
  no switchport

interface Ethernet2/38
```

```
  no switchport

interface Ethernet2/39
  no switchport

interface Ethernet2/40
  no switchport

interface Ethernet2/41
  no switchport

interface Ethernet2/42
  no switchport

interface Ethernet2/43
  no switchport

interface Ethernet2/44
  no switchport

interface Ethernet2/45
  no switchport

interface Ethernet2/46
  no switchport

interface Ethernet2/47
  no switchport

interface Ethernet2/48
  no switchport

interface loopback0
  vrf member servers1
  ip address 192.168.1.31/32
  ip router ospf 5 area 0.0.0.81
logging server 192.168.42.124 6 use-vrf servers1
logging source-interface loopback 0
  logout-warning 20
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
router ospf 5
  vrf servers1
    router-id 4.4.4.1
    area 0.0.0.81 nssa
    redistribute static route-map VLAN41
    area 0.0.0.81 range 192.168.0.0/16
    area 0.0.0.81 range 192.168.162.0/24
    area 0.0.0.81 authentication message-digest
    timers throttle spf 10 100 5000
  vrf servers2
    router-id 5.5.5.1
    area 0.0.0.81 nssa
    area 0.0.0.81 range 192.168.0.0/16
    area 0.0.0.81 range 192.168.152.0/24
    area 0.0.0.81 authentication message-digest
    timers throttle spf 10 100 5000
ip pim ssm range 232.0.0.0/8
```

RAGG-2-running

```
!Command: show running-config
!Time: Sun Apr 24 16:52:03 2011

version 5.1(2)
hostname RAGG-2
vdc RAGG-2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 32 maximum 32
  limit-resource u6route-mem minimum 16 maximum 16
  limit-resource m4route-mem minimum 48 maximum 48
  limit-resource m6route-mem minimum 8 maximum 8
vdc vdc1 id 2
  allocate interface Ethernet1/1,Ethernet1/3,Ethernet1/5,Ethernet1/7,Ethernet1/25-32
  allocate interface Ethernet2/1-12
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
vdc vdc2 id 3
  allocate interface Ethernet1/2,Ethernet1/4,Ethernet1/6,Ethernet1/8-24
  allocate interface Ethernet2/13-48
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5

feature privilege
feature tacacs+

username admin password 5 <removed> role network-admin
username retail password 5 <removed> role network-admin
username bart password 5 <removed> role network-admin
username emc-ncm password 5 <removed> role network-admin
enable secret 5 <removed>

banner motd @
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
```

```
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
@

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host RAGG-2 192.168.42.37
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.42.37/32
  20 permit ip 192.168.41.101/32 192.168.42.37/32
  30 permit ip 192.168.41.102/32 192.168.42.37/32
  40 permit ip 192.168.42.111/32 192.168.42.37/32
  50 permit ip 192.168.42.122/32 192.168.42.37/32
  60 permit ip 192.168.42.131/32 192.168.42.37/32
  70 permit ip 192.168.42.133/32 192.168.42.37/32
  80 permit ip 192.168.42.138/32 192.168.42.37/32
  90 permit ip 10.19.151.99/32 192.168.42.37/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.42.37/32
  20 deny ip any any
ip access-list copp-system-acl-bgp
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ipv6 access-list copp-system-acl-bgp6
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ip access-list copp-system-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
ip access-list copp-system-acl-glbp
  10 permit udp any eq 3222 224.0.0.0/24 eq 3222
ip access-list copp-system-acl-hsrp
  10 permit udp any 224.0.0.0/24 eq 1985
ip access-list copp-system-acl-icmp
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-acl-icmp6
  10 permit icmp any any echo-request
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-acl-icmp6-msgs
  10 permit icmp any any router-advertisement
  20 permit icmp any any router-solicitation
  30 permit icmp any any nd-na
  40 permit icmp any any nd-ns
  50 permit icmp any any mld-query
  60 permit icmp any any mld-report
  70 permit icmp any any mld-reduction
```

```
ip access-list copp-system-acl-igmp
  10 permit igmp any 224.0.0.0/3
ip access-list copp-system-acl-msdp
  10 permit tcp any gt 1024 any eq 639
  20 permit tcp any eq 639 any gt 1024
ip access-list copp-system-acl-ntp
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ipv6 access-list copp-system-acl-ntp6
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ip access-list copp-system-acl-ospf
  10 permit ospf any any
ipv6 access-list copp-system-acl-ospf6
  10 permit 89 any any
ip access-list copp-system-acl-pim
  10 permit pim any 224.0.0.0/24
  20 permit udp any any eq pim-auto-rp
ip access-list copp-system-acl-pim-reg
  10 permit pim any any
ipv6 access-list copp-system-acl-pim6
  10 permit 103 any ff02::d/128
  20 permit udp any any eq pim-auto-rp
ip access-list copp-system-acl-radius
  10 permit udp any any eq 1812
  20 permit udp any any eq 1813
  30 permit udp any any eq 1645
  40 permit udp any any eq 1646
  50 permit udp any eq 1812 any
  60 permit udp any eq 1813 any
  70 permit udp any eq 1645 any
  80 permit udp any eq 1646 any
ipv6 access-list copp-system-acl-radius6
  10 permit udp any any eq 1812
  20 permit udp any any eq 1813
  30 permit udp any any eq 1645
  40 permit udp any any eq 1646
  50 permit udp any eq 1812 any
  60 permit udp any eq 1813 any
  70 permit udp any eq 1645 any
  80 permit udp any eq 1646 any
ip access-list copp-system-acl-rip
  10 permit udp any 224.0.0.0/24 eq rip
ip access-list copp-system-acl-sftp
  10 permit tcp any any eq 115
  20 permit tcp any eq 115 any
ip access-list copp-system-acl-snmp
  10 permit udp any any eq snmp
  20 permit udp any any eq snmptrap
ip access-list copp-system-acl-ssh
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
ipv6 access-list copp-system-acl-ssh6
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
ip access-list copp-system-acl-tacacs
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
ipv6 access-list copp-system-acl-tacacs6
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
ip access-list copp-system-acl-telnet
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
ipv6 access-list copp-system-acl-telnet6
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
ip access-list copp-system-acl-tftp
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
ipv6 access-list copp-system-acl-tftp6
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
ip access-list copp-system-acl-traceroute
  10 permit icmp any any ttl-exceeded
  20 permit icmp any any port-unreachable
ip access-list copp-system-acl-undesirable
  10 permit udp any any eq 1434
ip access-list copp-system-acl-vpc
  10 permit udp any any eq 3200
ip access-list copp-system-acl-vrrp
  10 permit 112 any 224.0.0.0/24
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-bgp
  match access-group name copp-system-acl-bgp6
  match access-group name copp-system-acl-eigrp
  match access-group name copp-system-acl-igmp
  match access-group name copp-system-acl-msdp
  match access-group name copp-system-acl-ospf
  match access-group name copp-system-acl-ospf6
  match access-group name copp-system-acl-pim
  match access-group name copp-system-acl-pim6
  match access-group name copp-system-acl-rip
  match access-group name copp-system-acl-vpc
class-map type control-plane match-any copp-system-class-exception
  match exception ip option
  match exception ip icmp unreachable
  match exception ipv6 option
  match exception ipv6 icmp unreachable
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-glbp
  match access-group name copp-system-acl-hsrp
  match access-group name copp-system-acl-vrrp
  match access-group name copp-system-acl-icmp6-msgs
  match access-group name copp-system-acl-pim-reg
class-map type control-plane match-any copp-system-class-management
  match access-group name copp-system-acl-ftp
  match access-group name copp-system-acl-ntp
  match access-group name copp-system-acl-ntp6
  match access-group name copp-system-acl-radius
  match access-group name copp-system-acl-sftp
  match access-group name copp-system-acl-snmp
  match access-group name copp-system-acl-ssh
  match access-group name copp-system-acl-ssh6
  match access-group name copp-system-acl-tacacs
  match access-group name copp-system-acl-telnet
  match access-group name copp-system-acl-tftp
  match access-group name copp-system-acl-tftp6
  match access-group name copp-system-acl-radius6
  match access-group name copp-system-acl-tacacs6
  match access-group name copp-system-acl-telnet6
class-map type control-plane match-any copp-system-class-monitoring
  match access-group name copp-system-acl-icmp
  match access-group name copp-system-acl-icmp6
  match access-group name copp-system-acl-traceroute
class-map type control-plane match-any copp-system-class-normal
  match protocol arp
class-map type control-plane match-any copp-system-class-redirect
  match redirect dhcp-snoop
  match redirect arp-inspect
class-map type control-plane match-any copp-system-class-undesirable
  match access-group name copp-system-acl-undesirable
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 39600 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-important
    police cir 1060 kbps bc 1000 ms conform transmit violate drop
  class copp-system-class-management
    police cir 10000 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-normal
    police cir 680 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-redirect
    police cir 280 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-monitoring
    police cir 130 kbps bc 1000 ms conform transmit violate drop
  class copp-system-class-exception
    police cir 360 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-undesirable
    police cir 32 kbps bc 250 ms conform drop violate drop
  class class-default
    police cir 100 kbps bc 250 ms conform transmit violate drop
control-plane
  service-policy input copp-system-policy
snmp-server user admin network-admin auth md5 <removed> priv <removed> localizedkey
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
  ip route 0.0.0.0/0 192.168.42.1
vlan 1

interface mgmt0
  ip address 192.168.42.37/24
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
  logout-warning 20
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
boot kickstart bootflash:/n7000-s1-kickstart.5.1.2.bin sup-1
boot system bootflash:/n7000-s1-dk9.5.1.2.bin sup-1
boot kickstart bootflash:/n7000-s1-kickstart.5.1.2.bin sup-2
boot system bootflash:/n7000-s1-dk9.5.1.2.bin sup-2
logging server 192.168.42.124 6 use-vrf management
```

RAGG-2-vdc1-running

```
!Command: show running-config
!Time: Sun Apr 24 16:52:35 2011

version 5.1(2)
hostname vdc1

feature privilege
feature tacacs+
cfs eth distribute
feature ospf
feature pim
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature glbp
feature vpc

username admin password 5 <removed>   role vdc-admin
username retail password 5 <removed>   role vdc-admin
username emc-ncm password 5 <removed>   role vdc-admin
username bart password 5 <removed>   role vdc-admin
enable secret 5 <removed>

banner motd @
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
@

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    source-interface loopback0
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.1.12/32
  20 permit ip 192.168.41.101/32 192.168.1.12/32
  30 permit ip 192.168.41.102/32 192.168.1.12/32
  40 permit ip 192.168.42.111/32 192.168.1.12/32
  50 permit ip 192.168.42.122/32 192.168.1.12/32
  60 permit ip 192.168.42.131/32 192.168.1.12/32
  70 permit ip 192.168.42.133/32 192.168.1.12/32
  80 permit ip 192.168.42.138/32 192.168.1.12/32
  90 permit ip 10.19.151.99/32 192.168.1.12/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.1.12/32
  20 deny ip any any
snmp-server user admin vdc-admin auth md5 <removed> priv <removed> localizedkey
aaa authentication login default group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
vlan 1,3,151,161

interface Vlan1

interface Vlan3
  no shutdown
  ip address 192.168.10.62/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 3
  ip ospf hello-interval 1
  ip router ospf 5 area 0.0.0.0

interface Vlan151
  no shutdown
  ip address 192.168.152.4/24
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 10 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.152.1

interface Vlan161
  no shutdown
  ip address 192.168.162.4/24
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 10 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.162.1

interface port-channel99
  switchport
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/1
  description 10Gig LINK to RCORE-1 T2/2
  no switchport
  logging event port link-status
  no ip redirects
  ip address 192.168.10.18/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 6
  ip ospf hello-interval 2
  ip ospf network point-to-point
  ip router ospf 5 area 0.0.0.0
  ip pim sparse-mode
  ip igmp version 3
  no shutdown

interface Ethernet1/3
  description 10Gig LINK to RCORE-2 T2/2
  no switchport
  logging event port link-status
  no ip redirects
  ip address 192.168.10.26/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 6
  ip ospf hello-interval 2
  ip ospf network point-to-point
  ip router ospf 5 area 0.0.0.0
  ip pim sparse-mode
  ip igmp version 3
  no shutdown

interface Ethernet1/5
  description to DC-ASA-2 vc1 T0/6
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 161
  spanning-tree port type normal
  no shutdown

interface Ethernet1/7
  description to DC-ASA-2 vc2 T0/8
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 151
  spanning-tree port type normal
  no shutdown

interface Ethernet1/25
  no switchport

interface Ethernet1/26
  no switchport

interface Ethernet1/27
  no switchport

interface Ethernet1/28
  no switchport

interface Ethernet1/29
  description RAGG-1 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown
```

```
interface Ethernet1/30
  description RAGG-1 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet1/31
  description RAGG-1 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet1/32
  description RAGG-1 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet2/1
  no switchport

interface Ethernet2/2
  no switchport

interface Ethernet2/3
  no switchport

interface Ethernet2/4
  no switchport

interface Ethernet2/5
  no switchport

interface Ethernet2/6
  no switchport

interface Ethernet2/7
  no switchport

interface Ethernet2/8
  no switchport

interface Ethernet2/9
  no switchport

interface Ethernet2/10
  no switchport

interface Ethernet2/11
  no switchport

interface Ethernet2/12
  no switchport

interface loopback0
  ip address 192.168.1.12/32
  ip router ospf 5 area 0.0.0.0
logging server 192.168.42.124 6
logging source-interface loopback 0
  logout-warning 20
line console
```

```
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
router ospf 5
  router-id 192.168.1.12
  area 0.0.0.81 nssa
  area 0.0.0.0 range 192.168.1.12/32
  area 0.0.0.0 range 192.168.10.12/30
  area 0.0.0.0 range 192.168.10.20/30
  area 0.0.0.0 range 192.168.10.60/30
  area 0.0.0.81 range 192.168.152.0/24
  area 0.0.0.81 range 192.168.162.0/24
  area 0.0.0.0 authentication message-digest
  area 0.0.0.81 authentication message-digest
  timers throttle spf 10 100 5000
  auto-cost reference-bandwidth 10000
ip pim ssm range 232.0.0.0/8
```

RAGG-2-vdc2-running

```
!Command: show running-config
!Time: Sun Apr 24 16:53:03 2011

version 5.1(2)
hostname vdc2

feature privilege
feature tacacs+
cfs eth distribute
feature ospf
feature pim
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature dhcp
feature vpc

username admin password 5 <removed>   role vdc-admin
username retail password 5 <removed>   role vdc-admin
username bart password 5 <removed>   role vdc-admin
username emc-ncm password 5 <removed>   role vdc-admin
enable secret 5 <removed>

banner motd @
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
```

```
@

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
tacacs-server key 7 “<removed>”
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf servers1
    source-interface loopback0
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.1.32/32
  20 permit ip 192.168.41.101/32 192.168.1.32/32
  30 permit ip 192.168.41.102/32 192.168.1.32/32
  40 permit ip 192.168.42.111/32 192.168.1.32/32
  50 permit ip 192.168.42.122/32 192.168.1.32/32
  60 permit ip 192.168.42.131/32 192.168.1.32/32
  70 permit ip 192.168.42.133/32 192.168.1.32/32
  80 permit ip 192.168.42.138/32 192.168.1.32/32
  90 permit ip 10.19.151.99/32 192.168.1.32/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.1.32/32
  20 deny ip any any
snmp-server user admin vdc-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user retail vdc-admin auth md5 <removed> priv <removed> localizedkey
aaa authentication login default group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context VPC
vrf context servers1
  ip route 0.0.0.0/0 192.168.36.3
  ip pim ssm range 232.0.0.0/8
vrf context servers2
  ip pim ssm range 232.0.0.0/8
vrf context management
vlan 1
vlan 36
  name DeviceMgmtHigh
vlan 37
  name DeviceMgmtLow
vlan 38
  name UIM-OS-INSTALL
vlan 40-41
vlan 42
  name CoreManagement
vlan 43
  name WirelessSystems
vlan 44
  name PhysicalSec
vlan 45
  name VOICE
vlan 52
  name POS
vlan 151-152,154,161-162,164,180-181
spanning-tree domain 777
ip prefix-list VLAN41 seq 5 permit 192.168.41.0/24
route-map VLAN41 permit 20
```

```
  match ip address prefix-list VLAN41
service dhcp
ip dhcp relay
vpc domain 99
  peer-keepalive destination 192.168.10.65 source 192.168.10.66 vrf VPC


interface Vlan1
  no ip redirects
  no shutdown

interface Vlan36
  vrf member servers1
  no ip redirects
  ip address 192.168.36.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.36.1
  no shutdown
  description DeviceMgmtHigh

interface Vlan37
  vrf member servers1
  no ip redirects
  ip address 192.168.37.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.37.1
  no shutdown
  description DeviceMgmtLow

interface Vlan38
  vrf member servers1
  no ip redirects
  ip address 192.168.38.202/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  no shutdown
  description UIM OS Install only

interface Vlan40
  vrf member servers1
  no ip redirects
  ip address 192.168.40.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.40.1
  no shutdown

interface Vlan41
  vrf member servers1
  ip address 192.168.41.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 90 forwarding-threshold lower 1 upper 1
    timers  1  3
    ip 192.168.41.1
  shutdown
  description SHUTDOWN - NOW ROUTE VIA HyTrust

interface Vlan42
  vrf member servers1
  no ip redirects
  ip address 192.168.42.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.42.1
  no shutdown

interface Vlan43
  vrf member servers1
  no ip redirects
  ip address 192.168.43.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.43.1
  no shutdown
  description Wireless Systems

interface Vlan44
  vrf member servers1
  no ip redirects
  ip address 192.168.44.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
```

```
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 105 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.44.1
    no shutdown
    description Wireless Systems

  interface Vlan45
    vrf member servers1
    no ip redirects
    ip address 192.168.45.4/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 105 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.45.1
    no shutdown
    description VOICE

  interface Vlan52
    vrf member servers1
    no ip redirects
    ip address 192.168.52.4/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 105 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.52.1
    no shutdown
    description POS

  interface Vlan154
    vrf member servers2
    no ip redirects
    ip address 192.168.152.6/24
    ip ospf authentication message-digest
    ip ospf message-digest-key 1 md5 3 <removed>
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 120 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.152.7
    no shutdown

  interface Vlan164
    vrf member servers1
    no ip redirects
    ip address 192.168.162.6/24
    ip ospf authentication message-digest
    ip ospf message-digest-key 1 md5 3 <removed>
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 2
      authentication text c1sc0
      preempt delay minimum 180
      priority 110 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.162.7
    no shutdown

  interface Vlan180
    vrf member servers1
    no ip redirects
    ip address 192.168.180.4/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 1
      authentication text c1sc0
      preempt delay minimum 180
      priority 110 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.180.1
    no shutdown

  interface Vlan181
    vrf member servers2
    no ip redirects
    ip address 192.168.181.4/24
    ip ospf passive-interface
    ip router ospf 5 area 0.0.0.81
    ip pim sparse-mode
    ip igmp version 3
    hsrp 1
      authentication text c1sc0
      preempt delay minimum 180
      priority 120 forwarding-threshold lower 0 upper 0
      timers  1  3
      ip 192.168.181.1
    no shutdown

  interface port-channel1
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 38,41-42,44
    vpc 1

  interface port-channel2
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 38,41-42,44
    vpc 2

  interface port-channel3
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 38,41-45,52
    vpc 3
```

```
interface port-channel4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  vpc 4

interface port-channel11
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  spanning-tree port type edge trunk
  vpc 11

interface port-channel12
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  spanning-tree port type edge trunk
  vpc 12

interface port-channel99
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  spanning-tree port type network
  spanning-tree guard loop
  vpc peer-link

interface Ethernet1/2
  description F-UCS-1_E2/1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 11 mode active
  no shutdown

interface Ethernet1/4
  description F-UCS-1_E2/2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  spanning-tree port type normal
  channel-group 11 mode active
  no shutdown

interface Ethernet1/6
  description F-UCS-2_E2/1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 12 mode active
  no shutdown

interface Ethernet1/8
  description F-UCS-2_E2/2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 12 mode active
  no shutdown

interface Ethernet1/9
  description SACCESS-3 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 3 mode active
  no shutdown

interface Ethernet1/10
  description SACCESS-3 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 3 mode active
  no shutdown

interface Ethernet1/11
  description SACCESS-4 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 4 mode active
  no shutdown

interface Ethernet1/12
  description SACCESS-4 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 4 mode active
  no shutdown

interface Ethernet1/13
  description SACCESS-1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  channel-group 1 mode active
  no shutdown

interface Ethernet1/14
  description SACCESS-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  channel-group 2 mode active
  no shutdown

interface Ethernet1/15
  no switchport

interface Ethernet1/16
  no switchport

interface Ethernet1/17
  description to RSERV-2 T2/6
  switchport
  switchport mode trunk
  spanning-tree port type normal
  no shutdown

interface Ethernet1/18
  description to RSERV-2 T2/5
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 42,164
  no shutdown
```

```
interface Ethernet1/19
  description to DC-ASA-2 vc1 T5/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 152
  spanning-tree port type normal
  no shutdown

interface Ethernet1/20
  description to DC-ASA-2 vc2 T7/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 152
  spanning-tree port type normal
  no shutdown

interface Ethernet1/21
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/22
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/23
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/24
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet2/13
  description SACCESS-5 vPC Channel link
  switchport
  switchport mode trunk

interface Ethernet2/14
  description linkstate for vpc
  no switchport
  vrf member VPC
  ip address 192.168.10.66/30
  no shutdown
```

```
interface Ethernet2/15
  no switchport

interface Ethernet2/16
  no switchport

interface Ethernet2/17
  no switchport

interface Ethernet2/18
  no switchport

interface Ethernet2/19
  no switchport

interface Ethernet2/20
  no switchport

interface Ethernet2/21
  no switchport

interface Ethernet2/22
  no switchport

interface Ethernet2/23
  no switchport

interface Ethernet2/24
  no switchport

interface Ethernet2/25
  no switchport

interface Ethernet2/26
  no switchport

interface Ethernet2/27
  no switchport

interface Ethernet2/28
  no switchport

interface Ethernet2/29
  no switchport

interface Ethernet2/30
  no switchport

interface Ethernet2/31
  no switchport

interface Ethernet2/32
  no switchport

interface Ethernet2/33
  no switchport

interface Ethernet2/34
  no switchport

interface Ethernet2/35
  no switchport
```

```
interface Ethernet2/36
  no switchport

interface Ethernet2/37
  no switchport

interface Ethernet2/38
  no switchport

interface Ethernet2/39
  no switchport

interface Ethernet2/40
  no switchport

interface Ethernet2/41
  no switchport

interface Ethernet2/42
  no switchport

interface Ethernet2/43
  no switchport

interface Ethernet2/44
  no switchport

interface Ethernet2/45
  no switchport

interface Ethernet2/46
  no switchport

interface Ethernet2/47
  no switchport

interface Ethernet2/48
  no switchport

interface loopback0
  vrf member servers1
  ip address 192.168.1.32/32
  ip router ospf 5 area 0.0.0.81
logging server 192.168.42.124 6 use-vrf servers1
logging source-interface loopback 0
  logout-warning 20
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
router ospf 5
  vrf servers1
    router-id 4.4.4.2
    area 0.0.0.81 nssa
    area 0.0.0.81 range 192.168.0.0/16
    area 0.0.0.81 range 192.168.162.0/24
    area 0.0.0.81 authentication message-digest
    timers throttle spf 10 100 5000
  vrf servers2
    router-id 5.5.5.2
    area 0.0.0.81 nssa
    area 0.0.0.81 range 192.168.0.0/16
    area 0.0.0.81 range 192.168.152.0/24
    area 0.0.0.81 authentication message-digest
    timers throttle spf 10 100 5000
ip pim ssm range 232.0.0.0/8
```

rcore-1

```
!
! Last configuration change at 01:37:46 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:37:47 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname RCORE-1
!
boot-start-marker
boot system flash disk0:s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
boot-end-marker
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
ip wccp 61
ip wccp 62
!
!
!
no ip bootp server
```

```
ip multicast-routing
ip ssh version 2
ip scp server enable
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
ipv6 mfib hardware-switching replication-mode ingress
vtp domain CiscoRetail
vtp mode transparent
mls ip cef load-sharing full simple
no mls acl tcam share-global
mls netflow interface
mls cef error action freeze
password encryption aes
!
crypto pki trustpoint TP-self-signed-1104
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1104
 revocation-check none
 rsakeypair TP-self-signed-1104
!
!
crypto pki certificate chain TP-self-signed-1104
 certificate self-signed 01
  <removed>
  quit
!
!
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree pathcost method long
environment temperature-controlled
diagnostic bootup level minimal
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
redundancy
```

```
 main-cpu
  auto-sync running-config
 mode sso
!
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface Port-channel99
 ip address 192.168.10.29 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
 ip ospf dead-interval 6
 logging event link-status
!
interface GigabitEthernet1/1
 description to DC WAN_SWAN-3
 ip address 192.168.11.11 255.255.255.0
 standby 0 ip 192.168.11.10
 standby 0 priority 101
 standby 0 preempt
!
interface GigabitEthernet1/2
 no ip address
 shutdown
!
interface GigabitEthernet1/3
 no ip address
 shutdown
!
interface GigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 no ip address
 shutdown
!
interface GigabitEthernet1/6
 no ip address
 shutdown
!
interface GigabitEthernet1/7
 no ip address
 shutdown
!
interface GigabitEthernet1/8
 no ip address
 shutdown
!
interface GigabitEthernet1/9
```

```
 no ip address
 shutdown
!
interface GigabitEthernet1/10
 no ip address
 shutdown
!
interface GigabitEthernet1/11
 no ip address
 shutdown
!
interface GigabitEthernet1/12
 no ip address
 shutdown
!
interface GigabitEthernet1/13
 no ip address
 shutdown
!
interface GigabitEthernet1/14
 no ip address
 shutdown
!
interface GigabitEthernet1/15
 no ip address
 shutdown
!
interface GigabitEthernet1/16
 no ip address
 shutdown
!
interface GigabitEthernet1/17
 no ip address
 shutdown
!
interface GigabitEthernet1/18
 no ip address
 shutdown
!
interface GigabitEthernet1/19
 no ip address
 shutdown
!
interface GigabitEthernet1/20
 no ip address
 shutdown
!
interface GigabitEthernet1/21
 no ip address
 shutdown
!
interface GigabitEthernet1/22
 no ip address
 shutdown
!
interface GigabitEthernet1/23
 no ip address
 shutdown
!
interface GigabitEthernet1/24
 no ip address
 shutdown
!
interface GigabitEthernet1/25
```

```
 no ip address
 shutdown
!
interface GigabitEthernet1/26
 no ip address
 shutdown
!
interface GigabitEthernet1/27
 no ip address
 shutdown
!
interface GigabitEthernet1/28
 no ip address
 shutdown
!
interface GigabitEthernet1/29
 no ip address
 shutdown
!
interface GigabitEthernet1/30
 no ip address
 shutdown
!
interface GigabitEthernet1/31
 no ip address
 shutdown
!
interface GigabitEthernet1/32
 no ip address
 shutdown
!
interface GigabitEthernet1/33
 no ip address
 shutdown
!
interface GigabitEthernet1/34
 no ip address
 shutdown
!
interface GigabitEthernet1/35
 no ip address
 shutdown
!
interface GigabitEthernet1/36
 no ip address
 shutdown
!
interface GigabitEthernet1/37
 no ip address
 shutdown
!
interface GigabitEthernet1/38
 no ip address
 shutdown
!
interface GigabitEthernet1/39
 no ip address
 shutdown
!
interface GigabitEthernet1/40
 no ip address
 shutdown
!
interface GigabitEthernet1/41
```

```
 no ip address
 shutdown
!
interface GigabitEthernet1/42
 no ip address
 shutdown
!
interface GigabitEthernet1/43
 no ip address
 shutdown
!
interface GigabitEthernet1/44
 no ip address
 shutdown
!
interface GigabitEthernet1/45
 no ip address
 shutdown
!
interface GigabitEthernet1/46
 no ip address
 shutdown
!
interface GigabitEthernet1/47
 no ip address
 shutdown
!
interface GigabitEthernet1/48
 no ip address
 shutdown
!
interface TenGigabitEthernet2/1
 description 10Gig LINK to RAGG-1 T1/3
 ip address 192.168.10.13 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip igmp query-interval 125
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
 ip ospf dead-interval 6
 logging event link-status
!
interface TenGigabitEthernet2/2
 description 10Gig LINK to RAGG-2 T1/3
 ip address 192.168.10.17 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip igmp query-interval 125
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
 ip ospf dead-interval 6
 logging event link-status
!
interface TenGigabitEthernet2/3
 description 10Gig LINK to RCORE-2
 no ip address
 channel-group 99 mode active
!
```

```
interface TenGigabitEthernet2/4
 description 10Gig LINK to RCORE-2
 no ip address
 channel-group 99 mode active
!
interface TenGigabitEthernet2/5
 no ip address
 shutdown
!
interface TenGigabitEthernet2/6
 no ip address
 shutdown
!
interface TenGigabitEthernet2/7
 no ip address
 shutdown
!
interface TenGigabitEthernet2/8
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 5
 router-id 192.168.1.1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 nsf
 redistribute static subnets
 passive-interface default
 no passive-interface TenGigabitEthernet2/1
 no passive-interface TenGigabitEthernet2/2
 no passive-interface Port-channel99
 network 192.168.0.0 0.0.255.255 area 0
 default-information originate metric 20 metric-type 1
!
ip classless
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.11.60 name default-to-internet
ip route 10.10.0.0 255.255.0.0 192.168.11.1 name route-to-stores
ip route 10.10.0.0 255.255.255.0 192.168.11.60 name route-to-SP
ip route 10.10.1.0 255.255.255.0 192.168.11.2
ip route 10.10.2.0 255.255.255.0 192.168.11.3
ip route 10.10.110.1 255.255.255.255 192.168.11.2
ip route 10.10.110.2 255.255.255.255 192.168.11.3
ip route 10.10.126.1 255.255.255.255 192.168.11.2
ip route 10.10.126.2 255.255.255.255 192.168.11.3
ip route 10.10.254.0 255.255.255.0 192.168.11.3
ip route 10.10.255.0 255.255.255.0 192.168.11.2
ip route 192.168.1.111 255.255.255.255 192.168.11.2
ip route 192.168.1.112 255.255.255.255 192.168.11.3
ip route 192.168.20.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.21.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.22.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.23.0 255.255.255.0 192.168.11.60 name route-to-DMZ
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip pim send-rp-discovery scope 2
ip tacacs source-interface Loopback0
!
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps MAC-Notification change move threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
!
!
dial-peer cor custom
!
```

```
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
!
```

```
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
mac-address-table aging-time 480
!
end
```

rcore-2

```
!
! Last configuration change at 01:42:02 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:42:02 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname RCORE-2
!
boot-start-marker
boot system flash disk1:s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
boot-end-marker
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed> username bart privilege 15 secret 5
<removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
call-home
 no alert-group configuration
 no alert-group diagnostic
 no alert-group environment
 no alert-group inventory
 no alert-group syslog
ip wccp 61
ip wccp 62
!
!
!
no ip bootp server
ip multicast-routing
ip ssh version 2
ip scp server enable
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
ipv6 mfib hardware-switching replication-mode ingress
vtp domain CiscoRetail
vtp mode transparent
mls ip cef load-sharing full simple
no mls acl tcam share-global
mls netflow interface
mls cef error action freeze
password encryption aes
!
crypto pki trustpoint TP-self-signed-1051
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1051
 revocation-check none
 rsakeypair TP-self-signed-1051
!
!
crypto pki certificate chain TP-self-signed-1051
 certificate self-signed 01
  <removed>
  quit
!
!
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree pathcost method long
environment temperature-controlled
diagnostic bootup level minimal
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
```

```
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.2 255.255.255.255
!
interface Port-channel99
 description link between CORE's
 ip address 192.168.10.30 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
 ip ospf dead-interval 6
 logging event link-status
!
interface GigabitEthernet1/1
 description to DC WAN_SWAN-3/4
 ip address 192.168.11.12 255.255.255.0
 standby 0 ip 192.168.11.10
 standby 0 priority 99
 standby 0 preempt
!
interface GigabitEthernet1/2
 no ip address
 shutdown
!
interface GigabitEthernet1/3
 no ip address
 shutdown
!
interface GigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 no ip address
 shutdown
!
interface GigabitEthernet1/6
 no ip address
 shutdown
```

```
!
interface GigabitEthernet1/7
 no ip address
 shutdown
!
interface GigabitEthernet1/8
 no ip address
 shutdown
!
interface GigabitEthernet1/9
 no ip address
 shutdown
!
interface GigabitEthernet1/10
 no ip address
 shutdown
!
interface GigabitEthernet1/11
 no ip address
 shutdown
!
interface GigabitEthernet1/12
 no ip address
 shutdown
!
interface GigabitEthernet1/13
 no ip address
 shutdown
!
interface GigabitEthernet1/14
 no ip address
 shutdown
!
interface GigabitEthernet1/15
 no ip address
 shutdown
!
interface GigabitEthernet1/16
 no ip address
 shutdown
!
interface GigabitEthernet1/17
 no ip address
 shutdown
!
interface GigabitEthernet1/18
 no ip address
 shutdown
!
interface GigabitEthernet1/19
 no ip address
 shutdown
!
interface GigabitEthernet1/20
 no ip address
 shutdown
!
interface GigabitEthernet1/21
 no ip address
 shutdown
!
interface GigabitEthernet1/22
 no ip address
 shutdown
```

```
!
interface GigabitEthernet1/23
 no ip address
 shutdown
!
interface GigabitEthernet1/24
 no ip address
 shutdown
!
interface GigabitEthernet1/25
 no ip address
 shutdown
!
interface GigabitEthernet1/26
 no ip address
 shutdown
!
interface GigabitEthernet1/27
 no ip address
 shutdown
!
interface GigabitEthernet1/28
 no ip address
 shutdown
!
interface GigabitEthernet1/29
 no ip address
 shutdown
!
interface GigabitEthernet1/30
 no ip address
 shutdown
!
interface GigabitEthernet1/31
 no ip address
 shutdown
!
interface GigabitEthernet1/32
 no ip address
 shutdown
!
interface GigabitEthernet1/33
 no ip address
 shutdown
!
interface GigabitEthernet1/34
 no ip address
 shutdown
!
interface GigabitEthernet1/35
 no ip address
 shutdown
!
interface GigabitEthernet1/36
 no ip address
 shutdown
!
interface GigabitEthernet1/37
 no ip address
 shutdown
!
interface GigabitEthernet1/38
 no ip address
 shutdown
```

```
!
interface GigabitEthernet1/39
 no ip address
 shutdown
!
interface GigabitEthernet1/40
 no ip address
 shutdown
!
interface GigabitEthernet1/41
 no ip address
 shutdown
!
interface GigabitEthernet1/42
 no ip address
 shutdown
!
interface GigabitEthernet1/43
 no ip address
 shutdown
!
interface GigabitEthernet1/44
 no ip address
 shutdown
!
interface GigabitEthernet1/45
 no ip address
 shutdown
!
interface GigabitEthernet1/46
 no ip address
 shutdown
!
interface GigabitEthernet1/47
 no ip address
 shutdown
!
interface GigabitEthernet1/48
 no ip address
 shutdown
!
interface TenGigabitEthernet2/1
 description 10Gig LINK to RAGG-1 T1/4
 ip address 192.168.10.21 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip igmp query-interval 125
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
 ip ospf dead-interval 6
 logging event link-status
!
interface TenGigabitEthernet2/2
 description 10Gig LINK to RAGG-2 T1/4
 ip address 192.168.10.25 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip igmp query-interval 125
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
 ip ospf dead-interval 6
 logging event link-status
!
interface TenGigabitEthernet2/3
 description 10Gig LINK to RCORE-1
 no ip address
 channel-group 99 mode active
!
interface TenGigabitEthernet2/4
 description 10Gig LINK to RCORE-1
 no ip address
 channel-group 99 mode active
!
interface TenGigabitEthernet2/5
 no ip address
 shutdown
!
interface TenGigabitEthernet2/6
 no ip address
 shutdown
!
interface TenGigabitEthernet2/7
 no ip address
 shutdown
!
interface TenGigabitEthernet2/8
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 5
 router-id 192.168.1.2
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 nsf
 redistribute static subnets
 passive-interface default
 no passive-interface TenGigabitEthernet2/1
 no passive-interface TenGigabitEthernet2/2
 no passive-interface Port-channel99
 network 192.168.0.0 0.0.255.255 area 0
 default-information originate metric 22 metric-type 1
!
```

```
ip classless
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.11.60 name default-to-internet
ip route 10.10.0.0 255.255.0.0 192.168.11.1 name route-to-stores
ip route 10.10.0.0 255.255.255.0 192.168.11.60 name route-to-SP
ip route 10.10.1.0 255.255.255.0 192.168.11.2
ip route 10.10.2.0 255.255.255.0 192.168.11.3
ip route 10.10.110.1 255.255.255.255 192.168.11.2
ip route 10.10.110.2 255.255.255.255 192.168.11.3
ip route 10.10.126.1 255.255.255.255 192.168.11.2
ip route 10.10.126.2 255.255.255.255 192.168.11.3
ip route 10.10.254.0 255.255.255.0 192.168.11.3
ip route 10.10.255.0 255.255.255.0 192.168.11.2
ip route 192.168.20.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.21.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.22.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.23.0 255.255.255.0 192.168.11.60 name route-to-DMZ
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip pim send-rp-discovery scope 2
ip tacacs source-interface Loopback0
!
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps MAC-Notification change move threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131 timeout 5
tacacs-server directed-request
```

```
tacacs-server key 7 <removed>
!
!
control-plane
!
!
dial-peer cor custom
!
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
mac-address-table aging-time 480
!
end
```

rie-1

```
!
! Last configuration change at 01:06:14 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:06:15 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:06:15 PST Sat Apr 30 2011 by retail
upgrade fpd auto
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname RIE-1
!
boot-start-marker
boot system flash disk2:/c7200-advipservicesk9-mz.151-4.M.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
```

```
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PST recurring
ip source-route
ip cef
!
!
!
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip inspect audit-trail
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
!
password encryption aes
!
!
!
!
!
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-26793975
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-26793975
 revocation-check none
 rsakeypair TP-self-signed-26793975
!
!
crypto pki certificate chain TP-self-signed-26793975
 certificate self-signed 01
  <removed>
    quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
redundancy
!
```

```
!
ip ssh version 2
ip scp server enable
!
!
!
!
!
!
!
!
interface GigabitEthernet0/1
 description link to RIE-3 G1/1
 ip address 192.168.22.11 255.255.255.0
 standby 1 ip 192.168.22.10
 standby 1 priority 105
 standby 1 preempt
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 description link to RIE-4 G1/1
 no ip address
 shutdown
 duplex full
 speed 1000
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/3
 description Link to RSP-3 G0/2
 ip address 10.10.3.6 255.255.255.0
 ip access-group COARSE-FILTER-INTERNET-IN in
 ip access-group COARSE-FILTER-INTERNET-OUT out
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip route 0.0.0.0 0.0.0.0 10.10.3.1
ip route 10.10.0.0 255.255.0.0 192.168.22.1
ip route 10.10.0.0 255.255.255.0 10.10.3.1
ip route 10.10.4.0 255.255.255.0 192.168.22.12
ip route 192.168.0.0 255.255.0.0 192.168.22.1
ip tacacs source-interface GigabitEthernet0/1
!
ip access-list extended COARSE-FILTER-INTERNET-IN
 remark --------------------------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny   ip any 192.168.22.0 0.0.0.255 log
 remark -
 remark ---Allow remaining public internet traffic---
 permit ip any any
ip access-list extended COARSE-FILTER-INTERNET-OUT
 remark ---Block private networks from reaching Internet---
 remark ----------------------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny   ip any 192.168.22.0 0.0.0.255 log
 remark -
 remark ---Allow remaining traffic to Internet---
 remark The source address should be your ISP assigned IP’s
 permit ip <your ISP Public Block> any
!
logging esm config
logging trap debugging
logging source-interface GigabitEthernet0/1
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source GigabitEthernet0/1
```

```
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server host 192.168.42.124 remoteuser
!
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
 shutdown
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
```

```
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 stopbits 1
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 no exec
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
scheduler allocate 4000 200
ntp source GigabitEthernet0/1
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

rie-2

```
!
! Last configuration change at 01:07:38 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:07:38 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:07:38 PST Sat Apr 30 2011 by retail
upgrade fpd auto
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname RIE-2
!
boot-start-marker
boot system flash bootflash:/c7200p-advipservicesk9-mz.151-4.M.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PST recurring
ip source-route
ip cef
!
!
!
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 65535
login quiet-mode access-class 23
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
!
password encryption aes
!
!
!
!
!
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-26800067
```

```
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-26800067
 revocation-check none
 rsakeypair TP-self-signed-26800067
!
!
crypto pki certificate chain TP-self-signed-26800067
 certificate self-signed 01
  <removed>
    quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
redundancy
!
!
ip ssh version 2
ip scp server enable
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/1
 description RIE-3 port G1/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
!
interface FastEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 description RIE-4 port G1/2
 ip address 192.168.22.12 255.255.255.0
 standby 1 ip 192.168.22.10
 standby 1 priority 95
 standby 1 preempt
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/3
 description Link to RSP-4 G0/2
 ip address 10.10.4.6 255.255.255.0
 ip access-group COARSE-FILTER-INTERNET-IN in
 ip access-group COARSE-FILTER-INTERNET-OUT out
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
!
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip route 0.0.0.0 0.0.0.0 10.10.4.1
ip route 10.10.0.0 255.255.0.0 192.168.22.1
ip route 10.10.0.0 255.255.255.0 10.10.4.1
ip route 10.10.3.0 255.255.255.0 192.168.22.11
ip route 192.168.0.0 255.255.0.0 192.168.22.1
ip tacacs source-interface GigabitEthernet0/2
!
ip access-list extended COARSE-FILTER-INTERNET-IN
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny   ip any 192.168.22.0 0.0.0.255 log
 remark -
 remark ---Allow remaining public internet traffic---
 permit ip any any
ip access-list extended COARSE-FILTER-INTERNET-OUT
 remark ---Block private networks from reaching Internet---
 remark -------------------------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny   ip any 192.168.22.0 0.0.0.255 log
 remark -
 remark ---Allow remaining traffic to Internet---
 remark The source address should be your ISP assigned IP's
 permit ip <your ISP Public Block> any
!
logging esm config
logging alarm informational
logging trap debugging
logging source-interface GigabitEthernet0/2
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source GigabitEthernet0/2
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server host 192.168.42.124 remoteuser
!
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 stopbits 1
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 no exec
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
scheduler allocate 4000 200
ntp source GigabitEthernet0/2
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

RIE-3

```
!
! Last configuration change at 08:36:26 PSTDST Thu Apr 28 2011 by retail
! NVRAM config last updated at 22:33:54 PSTDST Wed Apr 27 2011 by retail
!
upgrade fpd auto
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname RIE-3
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 51200
enable secret 5 <removed>.
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
svclc multiple-vlan-interfaces
svclc module 3 vlan-group 21,82,83,85
svclc vlan-group 21  21
svclc vlan-group 82  82
svclc vlan-group 83  83
svclc vlan-group 85  85
firewall multiple-vlan-interfaces
firewall module 4 vlan-group 21,82,200,250,300
firewall vlan-group 200  22,2305-2307
firewall vlan-group 300  91,92
intrusion-detection module 2 management-port access-vlan 21
intrusion-detection module 2 data-port 1 trunk allowed-vlan 83,84
!
!
!
no ip bootp server
ip ssh version 2
ip scp server enable
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
mls cef error action freeze
password encryption aes
!
crypto pki trustpoint TP-self-signed-1014
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1014
 revocation-check none
 rsakeypair TP-self-signed-1014
!
!
crypto pki certificate chain TP-self-signed-1014
 certificate self-signed 01
  <removed>  quit
!
!
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
spanning-tree mode pvst
spanning-tree extend system-id
diagnostic bootup level minimal
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.122 log
```

```
access-list 88 deny   any log
access-list 101 permit gre host 192.168.21.91 host 128.107.147.109
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 21
 name fwsm_inside
!
vlan 22
 name fwsm_outside
!
vlan 82
 name fwsm_ace_outside
!
vlan 83
 name ace_IDSM
!
vlan 84
 name IDSM_DMZ-inside
!
vlan 85
 name ft_ace
!
vlan 91
 name fwsm_failover
!
vlan 92
 name fwsm_statelink
!
vlan 993
 name Management
!
vlan 995
 name DMZ_Management
!
vlan 2305
 name fwsm_EmailSecurityAppliance
!
vlan 2306
 name fwsm_EmailSecurityMgrAppliance
!
vlan 2307
 name fwsm_WebSecApp
!
!
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key ciscokey address 128.107.147.109
!
!
crypto ipsec transform-set to_fred esp-des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 128.107.147.109
 set transform-set to_fred
 match address 101
```

```
!
!
!
interface Tunnel0
 ip address 172.26.0.1 255.255.255.0
 tunnel source Vlan21
 tunnel destination 128.107.147.109
!
interface Port-channel99
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/1
 description RIE-1 G0/1
 switchport
 switchport access vlan 22
!
interface GigabitEthernet1/2
 description RIE-2 G0/1
 switchport
 switchport access vlan 22
!
interface GigabitEthernet1/3
 no ip address
!
interface GigabitEthernet1/4
 no ip address
!
interface GigabitEthernet1/5
 description ASA-IE-1 G0
 switchport
 switchport access vlan 21
!
interface GigabitEthernet1/6
 no ip address
!
interface GigabitEthernet1/7
 no ip address
!
interface GigabitEthernet1/8
 no ip address
!
interface GigabitEthernet1/9
 no ip address
!
interface GigabitEthernet1/10
 no ip address
!
interface GigabitEthernet1/11
 no ip address
!
interface GigabitEthernet1/12
 no ip address
!
interface GigabitEthernet1/13
 description ESA-IE-1 port M
 switchport
 switchport access vlan 2306
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/14
 description ESA-IE-1 port D1
 switchport
 switchport access vlan 2306
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/15
 description ESA-IE-1 port D2
 switchport
 switchport access vlan 2306
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/16
 description ESA-IE-1 port D3
 switchport
 switchport access vlan 2306
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/17
 description WSA-IE-1 port P1
 no ip address
!
interface GigabitEthernet1/18
 description WSA-IE-1 port P2
 no ip address
!
interface GigabitEthernet1/19
 description WSA-IE-1 port T1
 no ip address
!
interface GigabitEthernet1/20
 description WSA-IE-1 port T2
 no ip address
!
interface GigabitEthernet1/21
 description ESA-IE-1 port M
 switchport
 switchport access vlan 2305
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/22
 description ESA-IE-1 port D1
 switchport
 switchport access vlan 2305
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/23
 description ESA-IE-1 port D2
 switchport
 switchport access vlan 2305
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/24
 description ESA-IE-1 port D3
 switchport
 switchport access vlan 2305
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/25
```

```
 description WSA-IE-1 port M
 switchport
 switchport access vlan 2307
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/26
 no ip address
!
interface GigabitEthernet1/27
 no ip address
!
interface GigabitEthernet1/28
 no ip address
!
interface GigabitEthernet1/29
 no ip address
!
interface GigabitEthernet1/30
 no ip address
!
interface GigabitEthernet1/31
 no ip address
!
interface GigabitEthernet1/32
 no ip address
!
interface GigabitEthernet1/33
 no ip address
!
interface GigabitEthernet1/34
 no ip address
!
interface GigabitEthernet1/35
 no ip address
!
interface GigabitEthernet1/36
 no ip address
!
interface GigabitEthernet1/37
 no ip address
!
interface GigabitEthernet1/38
 no ip address
!
interface GigabitEthernet1/39
 no ip address
!
interface GigabitEthernet1/40
 no ip address
!
interface GigabitEthernet1/41
 no ip address
!
interface GigabitEthernet1/42
 no ip address
!
interface GigabitEthernet1/43
 no ip address
!
interface GigabitEthernet1/44
 no ip address
!
interface GigabitEthernet1/45
```

```
 no ip address
!
interface GigabitEthernet1/46
 no ip address
!
interface GigabitEthernet1/47
 no ip address
!
interface GigabitEthernet1/48
 no ip address
!
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 99 mode active
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 99 mode active
!
interface Vlan1
 no ip address
!
interface Vlan21
 description RIE-3 Management
 ip address 192.168.21.91 255.255.255.0
 crypto map myvpn
!
ip classless
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.21.10
ip route 10.10.0.0 255.255.0.0 192.168.21.1
ip route 10.10.0.0 255.255.252.0 192.168.21.10
ip route 10.10.192.0 255.255.240.0 172.26.0.2
ip route 192.168.0.0 255.255.0.0 192.168.21.1
ip route 192.168.23.0 255.255.255.0 192.168.21.10
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan21
!
logging trap debugging
logging source-interface Vlan21
logging 192.168.42.124
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  23
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
```

```
snmp-server enable traps hsrp
snmp-server enable traps MAC-Notification change move threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
!
!
dial-peer cor custom
!
!
!
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
```

```
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
!
scheduler allocate 20000 1000
ntp clock-period 17180154
ntp source Vlan21
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
end
```

RIE-4

```
!
! Last configuration change at 23:18:02 PSTDST Wed Apr 27 2011 by retail
! NVRAM config last updated at 23:18:04 PSTDST Wed Apr 27 2011 by retail
!
upgrade fpd auto
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log uptime
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname RIE-4
!
boot-start-marker
boot system flash disk0:s72033-adventerprisek9_wan-mz.122-33.SXI5.bin
boot-end-marker
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 51200
enable secret 5 <removed>
```

```
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
svclc multiple-vlan-interfaces
svclc module 3 vlan-group 82,83,85
svclc vlan-group 82  82
svclc vlan-group 83  83
svclc vlan-group 85  85
firewall multiple-vlan-interfaces
firewall vlan-group 200  21,22,2305-2307
firewall vlan-group 300  91,92
intrusion-detection module 2 management-port access-vlan 21
intrusion-detection module 2 data-port 1 trunk allowed-vlan 83,84
!
!
!
no ip bootp server
ip ssh version 2
ip scp server enable
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
ipv6 mfib hardware-switching replication-mode ingress
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
mls cef error action freeze
password encryption aes
!
crypto pki trustpoint TP-self-signed-1112
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1112
 revocation-check none
 rsakeypair TP-self-signed-1112
!
!
crypto pki certificate chain TP-self-signed-1112
 certificate self-signed 01
  <removed>  quit
!
!
!
!
!
```

```
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
spanning-tree mode pvst
spanning-tree extend system-id
diagnostic bootup level minimal
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.122 log
access-list 88 deny   any log
access-list 101 permit gre host 192.168.21.91 host 128.107.147.109
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 21
 name fwsm_inside
!
vlan 22
 name fwsm_outside
!
vlan 82
 name fwsm_ace_outside
!
vlan 83
 name ace_IDSM
!
vlan 84
 name IDSM_DMZ-inside
!
vlan 85
 name ft_ace
!
vlan 91
 name fwsm_failover
!
vlan 92
 name fwsm_statelink
!
vlan 993
 name Management
!
vlan 995
 name DMZ_Management
!
```

```
vlan 2305
 name fwsm_EmailSecurityAppliance
!
vlan 2306
 name fwsm_EmailSecurityMgrAppliance
!
vlan 2307
 name fwsm_WebSecApp
!
!
!
!
!
interface Port-channel99
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/1
 description RIE-1 G0/2
 switchport
 switchport access vlan 22
 shutdown
!
interface GigabitEthernet1/2
 description RIE-2 G0/2
 switchport
 switchport access vlan 22
!
interface GigabitEthernet1/3
 no ip address
 shutdown
!
interface GigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 description ASA-IE-2 G0
 switchport
 switchport access vlan 21
 shutdown
!
interface GigabitEthernet1/6
 no ip address
 shutdown
!
interface GigabitEthernet1/7
 no ip address
 shutdown
!
interface GigabitEthernet1/8
 no ip address
 shutdown
!
interface GigabitEthernet1/9
 no ip address
 shutdown
!
interface GigabitEthernet1/10
 no ip address
 shutdown
!
interface GigabitEthernet1/11
```

```
 no ip address
 shutdown
!
interface GigabitEthernet1/12
 no ip address
 shutdown
!
interface GigabitEthernet1/13
 description ESA-IE-2 port M
 switchport
 switchport access vlan 2306
 switchport mode access
 shutdown
!
interface GigabitEthernet1/14
 description ESA-IE-2 port D1
 switchport
 switchport access vlan 2306
 switchport mode access
 shutdown
!
interface GigabitEthernet1/15
 description ESA-IE-2 port D2
 switchport
 switchport access vlan 2306
 switchport mode access
 shutdown
!
interface GigabitEthernet1/16
 description ESA-IE-2 port D3
 switchport
 switchport access vlan 2306
 switchport mode access
 shutdown
!
interface GigabitEthernet1/17
 description WSA-IE-2 port P1
 no ip address
 shutdown
!
interface GigabitEthernet1/18
 description WSA-IE-2 port P2
 no ip address
 shutdown
!
interface GigabitEthernet1/19
 description WSA-IE-2 port T1
 no ip address
 shutdown
!
interface GigabitEthernet1/20
 description WSA-IE-2 port T2
 no ip address
 shutdown
!
interface GigabitEthernet1/21
 description ESA-IE-2 port M
 switchport
 switchport access vlan 2305
 switchport mode access
 shutdown
!
interface GigabitEthernet1/22
 description ESA-IE-2 port D1
 switchport
 switchport access vlan 2305
 switchport mode access
 shutdown
!
interface GigabitEthernet1/23
 description ESA-IE-2 port D2
 switchport
 switchport access vlan 2305
 switchport mode access
 shutdown
!
interface GigabitEthernet1/24
 description ESA-IE-2 port D3
 switchport
 switchport access vlan 2305
 switchport mode access
 shutdown
!
interface GigabitEthernet1/25
 description WSA-IE-2 port M
 switchport
 switchport access vlan 2307
 switchport mode access
!
interface GigabitEthernet1/26
 no ip address
 shutdown
!
interface GigabitEthernet1/27
 no ip address
 shutdown
!
interface GigabitEthernet1/28
 no ip address
 shutdown
!
interface GigabitEthernet1/29
 no ip address
 shutdown
!
interface GigabitEthernet1/30
 no ip address
 shutdown
!
interface GigabitEthernet1/31
 no ip address
 shutdown
!
interface GigabitEthernet1/32
 no ip address
 shutdown
!
interface GigabitEthernet1/33
 no ip address
 shutdown
!
interface GigabitEthernet1/34
 no ip address
 shutdown
!
interface GigabitEthernet1/35
 no ip address
 shutdown
```

```
!
interface GigabitEthernet1/36
 no ip address
 shutdown
!
interface GigabitEthernet1/37
 no ip address
 shutdown
!
interface GigabitEthernet1/38
 no ip address
 shutdown
!
interface GigabitEthernet1/39
 no ip address
 shutdown
!
interface GigabitEthernet1/40
 no ip address
 shutdown
!
interface GigabitEthernet1/41
 no ip address
 shutdown
!
interface GigabitEthernet1/42
 no ip address
 shutdown
!
interface GigabitEthernet1/43
 no ip address
 shutdown
!
interface GigabitEthernet1/44
 no ip address
 shutdown
!
interface GigabitEthernet1/45
 no ip address
 shutdown
!
interface GigabitEthernet1/46
 no ip address
 shutdown
!
interface GigabitEthernet1/47
 no ip address
 shutdown
!
interface GigabitEthernet1/48
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 99 mode active
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 99 mode active
```

```
!
interface Vlan1
 no ip address
!
interface Vlan21
 description RIE-3 Management
 ip address 192.168.21.92 255.255.255.0
!
ip classless
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.21.10
ip route 10.10.0.0 255.255.0.0 192.168.21.1
ip route 10.10.0.0 255.255.252.0 192.168.21.10
ip route 10.10.192.0 255.255.240.0 172.26.0.2
ip route 192.168.0.0 255.255.0.0 192.168.21.1
ip route 192.168.23.0 255.255.255.0 192.168.21.10
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
logging trap debugging
logging source-interface Vlan21
logging 192.168.42.124
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  23
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps MAC-Notification change move threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
```

```
!
!
dial-peer cor custom
!
!
!
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
```

```
!
ntp clock-period 17179993
ntp source Vlan21
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
end
```

rserv-1

```
!
! Last configuration change at 01:53:06 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:53:07 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname RSERV-1
!
boot-start-marker
boot system flash sup-bootdisk:/s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
boot-end-marker
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
svclc module 4 vlan-group 162,163
svclc vlan-group 162  152,162
svclc vlan-group 163  153,163
```

```
intrusion-detection module 9 management-port access-vlan 42
intrusion-detection module 9 data-port 1 trunk allowed-vlan 153,154
intrusion-detection module 9 data-port 2 trunk allowed-vlan 163,164
ip wccp 61
ip wccp 62
!
!
!
no ip bootp server
ip multicast-routing
ip ssh version 2
ip scp server enable
no ip domain-lookup
ip domain-name cisco-irn.com
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
ipv6 mfib hardware-switching replication-mode ingress
vtp domain datacenter
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
mls cef error action freeze
password encryption aes
!
crypto pki trustpoint TP-self-signed-1027
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1027
 revocation-check none
 rsakeypair TP-self-signed-1027
!
!
crypto pki certificate chain TP-self-signed-1027
 certificate self-signed 01
  <removed>
  quit
!
!
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
spanning-tree mode pvst
!
no power enable module 8
diagnostic bootup level minimal
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
```

```
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 41
 name DeviceManagementHTA
!
vlan 42
 name DeviceManagement
!
vlan 43
 name WIRELESS-CONTROL
!
vlan 44
 name PhysicalSec
!
vlan 47
 name WAAS_Central_Manager
!
vlan 49
 name WAAS_DC
!
vlan 152
 name NorthSide_facing_ASA_Servers2
!
vlan 153
 name ACE_to_IDS_Servers2
!
vlan 154
 name SouthSide_facing_Servers2
!
vlan 162
 name NorthSide_facing_ASA_Servers1
!
vlan 163
 name ACE_to_IDS_Servers1
!
vlan 164
 name SouthSide_facing_Servers1
!
vlan 803
 name RSERV-1_to_RAGG-1-VDC-2
!
vlan 1000
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.21 255.255.255.255
!
interface Loopback62
 ip address 192.168.62.161 255.255.255.255
```

```
!
interface GigabitEthernet1/1
 no ip address
 shutdown
!
interface GigabitEthernet1/2
 no ip address
 shutdown
!
interface GigabitEthernet1/3
 no ip address
 shutdown
!
interface GigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 no ip address
 shutdown
!
interface GigabitEthernet1/6
 no ip address
 shutdown
!
interface GigabitEthernet1/7
 no ip address
 shutdown
!
interface GigabitEthernet1/8
 no ip address
 shutdown
!
interface GigabitEthernet1/9
 no ip address
 shutdown
!
interface GigabitEthernet1/10
 no ip address
 shutdown
!
interface GigabitEthernet1/11
 no ip address
 shutdown
!
interface GigabitEthernet1/12
 no ip address
 shutdown
!
interface GigabitEthernet1/13
 no ip address
 shutdown
!
interface GigabitEthernet1/14
 no ip address
 shutdown
!
interface GigabitEthernet1/15
 no ip address
 shutdown
!
interface GigabitEthernet1/16
 no ip address
 shutdown
```

```
!
interface TenGigabitEthernet2/1
 description to RAGG-1 vdc2 T1/15
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 162
 switchport mode trunk
!
interface TenGigabitEthernet2/2
 description to RAGG-1 vdc2 T1/16
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 152
 switchport mode trunk
!
interface TenGigabitEthernet2/3
 no ip address
 shutdown
!
interface TenGigabitEthernet2/4
 no ip address
 shutdown
!
interface TenGigabitEthernet2/5
 description to RAGG-1 vdc2 T1/17
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 41-44,164,803
 switchport mode trunk
!
interface TenGigabitEthernet2/6
 description to RAGG-1 vdc2 T1/18
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 154
 switchport mode trunk
!
interface TenGigabitEthernet2/7
 no ip address
 shutdown
!
interface TenGigabitEthernet2/8
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 no ip address
 shutdown
!
interface GigabitEthernet7/1
 no ip address
 shutdown
```

```
!
interface GigabitEthernet7/2
 no ip address
 shutdown
!
interface GigabitEthernet7/3
 no ip address
!
interface GigabitEthernet7/4
 no ip address
!
interface GigabitEthernet7/5
 no ip address
!
interface GigabitEthernet7/6
 no ip address
!
interface GigabitEthernet7/7
 no ip address
!
interface GigabitEthernet7/8
 no ip address
!
interface GigabitEthernet7/9
 no ip address
!
interface GigabitEthernet7/10
 no ip address
!
interface GigabitEthernet7/11
 no ip address
!
interface GigabitEthernet7/12
 no ip address
!
interface GigabitEthernet7/13
 no ip address
!
interface GigabitEthernet7/14
 no ip address
!
interface GigabitEthernet7/15
 no ip address
!
interface GigabitEthernet7/16
 no ip address
!
interface GigabitEthernet7/17
 description WAAS Central Manager
 switchport
 switchport access vlan 47
 switchport mode access
!
interface GigabitEthernet7/18
 no ip address
!
interface GigabitEthernet7/19
 no ip address
!
interface GigabitEthernet7/20
 no ip address
!
interface GigabitEthernet7/21
 description AW-DC-1_G1
 switchport
 switchport access vlan 43
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/22
 description AW-DC-2_G1
 switchport
 switchport access vlan 43
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/23
 description MDS Management PAME-DC-1
 switchport
 switchport access vlan 44
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/24
 description MDS Management MDS-DC-1_M0
 switchport
 switchport access vlan 41
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/25
 description MDS Management MDS-DC-2_M0
 switchport
 switchport access vlan 41
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/26
 no ip address
!
interface GigabitEthernet7/27
 description ASA-WAN-1_M0
 switchport
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/28
 no ip address
!
interface GigabitEthernet7/29
 description MSE-DC-1_G1
 switchport
 switchport access vlan 43
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/30
 description MSE-DC-2_G1
 switchport
 switchport access vlan 43
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/31
 no ip address
!
interface GigabitEthernet7/32
```

```
 no ip address
!
interface GigabitEthernet7/33
 description RSA enVision
 switchport
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/34
 no ip address
!
interface GigabitEthernet7/35
 description WAE-DC-1
 switchport
 switchport access vlan 49
 switchport mode access
!
interface GigabitEthernet7/36
 no ip address
!
interface GigabitEthernet7/37
 no ip address
!
interface GigabitEthernet7/38
 no ip address
!
interface GigabitEthernet7/39
 no ip address
!
interface GigabitEthernet7/40
 no ip address
!
interface GigabitEthernet7/41
 no ip address
!
interface GigabitEthernet7/42
 no ip address
!
interface GigabitEthernet7/43
 no ip address
!
interface GigabitEthernet7/44
 no ip address
!
interface GigabitEthernet7/45
 description hard crossover bridge
 no ip address
 shutdown
!
interface GigabitEthernet7/46
 no ip address
!
interface GigabitEthernet7/47
 no ip address
 shutdown
!
interface GigabitEthernet7/48
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
```

```
!
interface Vlan803
 description ** South Side facing Servers1 **
 ip address 192.168.130.10 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf priority 0
!
router ospf 5
 router-id 192.168.1.21
 log-adjacency-changes
 area 81 authentication message-digest
 area 81 nssa
 area 81 range 192.168.0.0 255.255.0.0
 timers throttle spf 10 100 5000
 passive-interface default
 no passive-interface Vlan803
 network 192.168.0.0 0.0.255.255 area 81
!
ip classless
no ip forward-protocol nd
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Loopback0
!
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps MAC-Notification change move threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps errdisable
```

```
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
!
!
dial-peer cor custom
!
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
```

```
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
!
ntp source Loopback0
ntp master 5
ntp update-calendar
ntp server 171.68.10.150
ntp server 171.68.10.80 prefer
mac-address-table aging-time 480
!
end
```

rserv-2

```
!
! Last configuration change at 01:50:12 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:50:13 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname RSERV-2
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
svclc module 4 vlan-group 162,163
svclc vlan-group 162  152,162
svclc vlan-group 163  153,163
intrusion-detection module 9 management-port access-vlan 42
intrusion-detection module 9 data-port 1 trunk allowed-vlan 153,154
intrusion-detection module 9 data-port 2 trunk allowed-vlan 163,164
ip wccp 61
ip wccp 62
!
!
!
no ip bootp server
ip multicast-routing
ip ssh version 2
ip scp server enable
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
ipv6 mfib hardware-switching replication-mode ingress
vtp domain CiscoRetail
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
mls cef error action freeze
password encryption aes
!
crypto pki trustpoint TP-self-signed-1027
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1027
 revocation-check none
 rsakeypair TP-self-signed-1027
!
!
crypto pki certificate chain TP-self-signed-1027
 certificate self-signed 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  2B312930 27060355 04031320 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31303237 301E170D 31313034 32313030 30353139 5A170D32
  30303130 31303030 3030305A 302B3129 30270603 55040313 20494F53 2D53656C
  662D5369 676E6564 2D436572 74696669 63617465 2D313032 3730819F 300D0609
  2A864886 F70D0101 01050003 818D0030 81890281 8100A365 80CA486A 1FCC3F72
  4B6DDFE1 AA57CE0A 4726554C B0D6B6F3 BC9F3F3A 84AAD96D 0C8D4E07 3E5C42FD
  2AB0BA8A 1E5E28AE BDA4FE3A F1A425A6 2D2F09E0 3DC30109 F4561A9B EADC4896
  87FD5133 4FEAFA2F C214CB35 11B7AEB6 F0C3DE4F 4453DA89 6177A6D3 9FDA59BA
  EE11414E 008C40A8 FF768B0D 0CE97204 82FB71C6 10C30203 010001A3 75307330
  0F060355 1D130101 FF040530 030101FF 30200603 551D1104 19301782 15525345
  52562D32 2E636973 636F2D69 726E2E63 6F6D301F 0603551D 23041830 16801425
  E9402754 9D8FF072 B2B9284C D1157536 23A79C30 1D060355 1D0E0416 041425E9
  4027549D 8FF072B2 B9284CD1 15753623 A79C300D 06092A86 4886F70D 01010405
  00038181 003EACB3 84C4E98F 65FE3BE2 F4984B3D 908DCF32 E89B4217 6F3444EB
  E844C491 A50B817E 508BE874 E4C1FE1E 9A92EDC5 8566CC69 AB760674 E802086B
  DDD7DF6A 3964355C 0F88B1AB 52E69373 D25A2877 3379ECAF A8D3DAE8 239C2708
  8B1C24DF 4210091C 8C3DF041 7B10147C E399480E 6A7D00DD 64D8AD86 528815E4
  7FAECE3C 2B
  quit
!
!
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
spanning-tree mode pvst
!
no power enable module 8
diagnostic bootup level minimal
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 41
 name DeviceManagementHTA
!
vlan 42
 name DeviceManagement
!
vlan 43
 name WIRELESS-CONTROL
!
vlan 44
 name PhysicalSec
!
vlan 47
 name WAAS_Central_Manager
!
vlan 49
 name WAAS_DC
!
vlan 152
 name NorthSide_facing_ASA_Servers2
!
```

```
vlan 153
 name ACE_to_IDS_Servers2
!
vlan 154
 name SouthSide_facing_Servers2
!
vlan 162
 name NorthSide_facing_ASA_Servers1
!
vlan 163
 name ACE_to_IDS_Servers1
!
vlan 164
 name SouthSide_facing_Servers1
!
vlan 804
 name RSERV-2_to_RAGG-2-VDC-2
!
vlan 1000
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.22 255.255.255.255
!
interface Loopback62
 ip address 192.168.62.162 255.255.255.255
!
interface GigabitEthernet1/1
 no ip address
 shutdown
!
interface GigabitEthernet1/2
 no ip address
 shutdown
!
interface GigabitEthernet1/3
 no ip address
 shutdown
!
interface GigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 no ip address
 shutdown
!
interface GigabitEthernet1/6
 no ip address
 shutdown
!
interface GigabitEthernet1/7
 no ip address
 shutdown
!
interface GigabitEthernet1/8
 no ip address
 shutdown
!
interface GigabitEthernet1/9
 no ip address
 shutdown
!
interface GigabitEthernet1/10
 no ip address
 shutdown
!
interface GigabitEthernet1/11
 no ip address
 shutdown
!
interface GigabitEthernet1/12
 no ip address
 shutdown
!
interface GigabitEthernet1/13
 no ip address
 shutdown
!
interface GigabitEthernet1/14
 no ip address
 shutdown
!
interface GigabitEthernet1/15
 no ip address
 shutdown
!
interface GigabitEthernet1/16
 no ip address
 shutdown
!
interface TenGigabitEthernet2/1
 description to RAGG-2 vdc2 T1/15
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 162
 switchport mode trunk
!
interface TenGigabitEthernet2/2
 description to RAGG-2 vdc2 T1/16
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 152
 switchport mode trunk
!
interface TenGigabitEthernet2/3
 no ip address
 shutdown
!
interface TenGigabitEthernet2/4
 no ip address
 shutdown
!
interface TenGigabitEthernet2/5
 description to RAGG-2 vdc2 T1/18
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 41-44,164,804
 switchport mode trunk
!
interface TenGigabitEthernet2/6
 description to RAGG-2 vdc2 T1/17
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 154
 switchport mode trunk
!
interface TenGigabitEthernet2/7
 no ip address
 shutdown
!
interface TenGigabitEthernet2/8
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 no ip address
 shutdown
!
interface GigabitEthernet7/1
 switchport
 switchport access vlan 42
!
interface GigabitEthernet7/2
 no ip address
!
interface GigabitEthernet7/3
 no ip address
!
interface GigabitEthernet7/4
 no ip address
!
interface GigabitEthernet7/5
 description WAE-DC-2
 switchport
 switchport access vlan 48
 switchport mode access
!
interface GigabitEthernet7/6
 no ip address
!
interface GigabitEthernet7/7
 no ip address
!
interface GigabitEthernet7/8
 no ip address
!
interface GigabitEthernet7/9
 no ip address
!
interface GigabitEthernet7/10
 no ip address
!
interface GigabitEthernet7/11
 no ip address
!
interface GigabitEthernet7/12
```

```
 no ip address
!
interface GigabitEthernet7/13
 no ip address
!
interface GigabitEthernet7/14
 no ip address
!
interface GigabitEthernet7/15
 no ip address
!
interface GigabitEthernet7/16
 no ip address
!
interface GigabitEthernet7/17
 no ip address
!
interface GigabitEthernet7/18
 no ip address
!
interface GigabitEthernet7/19
 no ip address
!
interface GigabitEthernet7/20
 no ip address
!
interface GigabitEthernet7/21
 no ip address
!
interface GigabitEthernet7/22
 no ip address
!
interface GigabitEthernet7/23
 description PAME-DC-1
 switchport
 switchport access vlan 44
 switchport mode access
!
interface GigabitEthernet7/24
 no ip address
!
interface GigabitEthernet7/25
 no ip address
!
interface GigabitEthernet7/26
 no ip address
!
interface GigabitEthernet7/27
 description ASA-WAN-2_M0
 switchport
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/28
 no ip address
!
interface GigabitEthernet7/29
 no ip address
!
interface GigabitEthernet7/30
 no ip address
!
interface GigabitEthernet7/31
```

```
 no ip address
!
interface GigabitEthernet7/32
 no ip address
!
interface GigabitEthernet7/33
 no ip address
!
interface GigabitEthernet7/34
 no ip address
!
interface GigabitEthernet7/35
 no ip address
!
interface GigabitEthernet7/36
 no ip address
!
interface GigabitEthernet7/37
 no ip address
!
interface GigabitEthernet7/38
 no ip address
!
interface GigabitEthernet7/39
 no ip address
!
interface GigabitEthernet7/40
 no ip address
!
interface GigabitEthernet7/41
 no ip address
!
interface GigabitEthernet7/42
 no ip address
!
interface GigabitEthernet7/43
 no ip address
!
interface GigabitEthernet7/44
 no ip address
!
interface GigabitEthernet7/45
 no ip address
!
interface GigabitEthernet7/46
 no ip address
!
interface GigabitEthernet7/47
 no ip address
!
interface GigabitEthernet7/48
 no ip address
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan42
 ip address 192.168.42.47 255.255.255.0
!
interface Vlan804
 description ** South Side facing Servers1 **
 ip address 192.168.130.14 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf priority 0
!
router ospf 5
 router-id 192.168.1.22
 log-adjacency-changes
 area 81 authentication message-digest
 area 81 nssa
 area 81 range 192.168.0.0 255.255.0.0
 timers throttle spf 10 100 5000
 passive-interface default
 no passive-interface Vlan804
 network 192.168.0.0 0.0.255.255 area 81
!
ip classless
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.42.1 255 name backup_default
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Loopback0
!
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps MAC-Notification change move threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
```

```
!
!
control-plane
!
!
dial-peer cor custom
!
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
!
ntp source Loopback0
ntp master 5
ntp update-calendar
ntp server 171.68.10.150
ntp server 171.68.10.80 prefer
mac-address-table aging-time 480
!
end
```

rwan-1

```
!
! Last configuration change at 01:17:13 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:17:14 PSTDST Sat Apr 30 2011 by retail
!
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
no platform punt-keepalive disable-kernel-core
!
hostname RWAN-1
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 4 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
!
!
aaa session-id common
!
!
!
clock timezone PST -8 0
clock summer-time PSTDST recurring
ip source-route
!
!
!
no ip bootp server
no ip domain lookup
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip multicast-routing distributed
!
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
!
!
multilink bundle-name authenticated
!
password encryption aes
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-1264044905
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1264044905
 revocation-check none
 rsakeypair TP-self-signed-1264044905
!
!
crypto pki certificate chain TP-self-signed-1264044905
 certificate self-signed 01
  <removed>   quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
username retail privilege 15 secret 4 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 4 <removed>
username bmcgloth privilege 15 secret 4 <removed>
username csmadmin privilege 15 secret 4 <removed>
!
redundancy
```

```
 mode none
!
!
!
ip ssh version 2
ip scp server enable
!
class-map match-all BRANCH-BULK-DATA
 match access-group name BULK-DATA-APPS
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol telnet
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol dns
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
policy-map DataCenter-LAN-EDGE-OUT
 class class-default
policy-map DataCenter-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
policy-map DataCenter-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 1
  random-detect dscp-based
 class class-default
  bandwidth percent 25
  random-detect
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.111 255.255.255.255
!
interface GigabitEthernet0/0/0
 description SWAN-1
 ip address 192.168.11.2 255.255.255.0
 standby 1 ip 192.168.11.1
 standby 1 priority 105
 standby 1 preempt
 no negotiation auto
 service-policy input DataCenter-LAN-EDGE-IN
 service-policy output DataCenter-LAN-EDGE-OUT
!
interface GigabitEthernet0/0/1
 no ip address
 no negotiation auto
!
interface GigabitEthernet0/0/2
 description RSP-1 G0/1
 ip address 10.10.1.6 255.255.255.0
 no negotiation auto
 service-policy output DataCenter-WAN-EDGE
!
interface GigabitEthernet0/0/3
 no ip address
 shutdown
 no negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip route 0.0.0.0 0.0.0.0 192.168.11.60
ip route 10.10.0.0 255.255.0.0 10.10.1.1
ip route 10.10.0.0 255.255.0.0 192.168.11.3 50
ip route 10.10.0.0 255.255.255.0 192.168.11.60
ip route 10.10.2.0 255.255.255.0 192.168.11.3
ip route 10.10.3.0 255.255.255.0 192.168.11.60
ip route 10.10.4.0 255.255.255.0 192.168.11.60
ip route 10.10.110.2 255.255.255.255 192.168.11.3
ip route 10.10.126.2 255.255.255.255 192.168.11.3
ip route 10.10.254.0 255.255.255.0 192.168.11.3
ip route 192.168.0.0 255.255.0.0 192.168.11.10
ip route 192.168.1.112 255.255.255.255 192.168.11.3
ip route 192.168.20.0 255.255.252.0 192.168.11.60
ip route 192.168.24.0 255.255.255.0 192.168.11.60
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip 192.168.52.0 0.0.0.255 any
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 192.168.46.72 eq 8444 host 10.10.49.94
 remark --Large store Clock Server to CUAE
 permit tcp host 192.168.45.185 eq 8000 host 10.10.49.94
 remark ---LiteScape Application---
 permit ip host 192.168.46.82 any
 permit ip 239.192.0.0 0.0.0.255 any
 permit ip host 239.255.255.250 any
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
```

```
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
cdp run
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server enable traps flash insertion removal
snmp-server host 192.168.42.124 remoteuser
!
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
```

```
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 stopbits 1
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 no exec
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 17186047
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

rwan-2

```
!
! Last configuration change at 01:31:03 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:31:04 PST Sat Apr 30 2011 by retail
!
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
no platform punt-keepalive disable-kernel-core
!
hostname RWAN-2
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
!
!
aaa session-id common
!
!
!
clock timezone PST -8 0
clock summer-time PST recurring
ip source-route
!
!
!
no ip bootp server
no ip domain lookup
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip multicast-routing distributed
!
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
!
!
multilink bundle-name authenticated
```

```
!
password encryption aes
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-1414178861
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1414178861
 revocation-check none
 rsakeypair TP-self-signed-1414178861
!
!
crypto pki certificate chain TP-self-signed-1414178861
 certificate self-signed 01
  <removed>
    quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
username retail privilege 15 secret 4 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 4 <removed>
username bmcgloth privilege 15 secret 4 <removed>
username csmadmin privilege 15 secret 4 <removed>
!
redundancy
 mode none
!
!
!
ip ssh version 2
ip scp server enable
!
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.112 255.255.255.255
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/0/0
 description SWAN-2
 ip address 192.168.11.3 255.255.255.0
 standby 1 ip 192.168.11.1
 standby 1 priority 95
 no negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 no negotiation auto
!
interface GigabitEthernet0/0/2
 description RSP-2 G0/1
 ip address 10.10.2.6 255.255.255.0
 no negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 no negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip route 0.0.0.0 0.0.0.0 192.168.11.60
ip route 10.10.0.0 255.255.0.0 10.10.2.1
ip route 10.10.0.0 255.255.0.0 192.168.11.2 50
ip route 10.10.0.0 255.255.255.0 192.168.11.60
ip route 10.10.1.0 255.255.255.0 192.168.11.2
ip route 10.10.3.0 255.255.255.0 192.168.11.60
ip route 10.10.4.0 255.255.255.0 192.168.11.60
ip route 10.10.110.1 255.255.255.255 192.168.11.2
ip route 10.10.126.1 255.255.255.255 192.168.11.2
ip route 10.10.255.0 255.255.255.0 192.168.11.2
ip route 192.168.0.0 255.255.0.0 192.168.11.10
ip route 192.168.1.111 255.255.255.255 192.168.11.2
ip route 192.168.20.0 255.255.252.0 192.168.11.60
ip route 192.168.24.0 255.255.255.0 192.168.11.60
ip tacacs source-interface Loopback0
!
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
```

```
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server enable traps flash insertion removal
snmp-server host 192.168.42.124 remoteuser
!
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 stopbits 1
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication RETAIL
 no exec
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 17219603
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

S-A2-Conv-1

```
Building configuration...

Current configuration : 8808 bytes
!
! Last configuration change at 02:11:23 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:11:23 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname S-A2-Conv-1
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!
```

```
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-3179870208
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3179870208
 revocation-check none
 rsakeypair TP-self-signed-3179870208
!
!
crypto pki certificate chain TP-self-signed-3179870208
 certificate self-signed 01
  <removed>
  quit
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet0/1
 switchport mode trunk
```

```
!
interface FastEthernet0/2
 description AIR-CAP1042N
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.175.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.175.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131 timeout 5
tacacs-server directed-request
tacacs-server key 7 <removed>
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36028799
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

S-A2-Lrg-1

```
S-A2-LRG-1#sh run
Building configuration...

Current configuration : 21232 bytes
!
! Last configuration change at 02:39:20 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:39:22 PSTDST Sat Apr 30 2011 by retail
!
version 15.0
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service compress-config
service sequence-numbers
!
hostname S-A2-LRG-1
!
boot-start-marker
boot system flash bootflash:cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
boot-end-marker
!
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
ip subnet-zero
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
!
no ip bootp server
ip vrf Mgmt-vrf
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
vtp mode transparent
!
password encryption aes
!
crypto pki trustpoint CISCO_IDEVID_SUDI
 revocation-check none
 rsakeypair CISCO_IDEVID_SUDI
!
crypto pki trustpoint CISCO_IDEVID_SUDI0
 revocation-check none
!
crypto pki trustpoint TP-self-signed-145264
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-145264
 revocation-check none
 rsakeypair TP-self-signed-145264
!
!
crypto pki certificate chain CISCO_IDEVID_SUDI
 certificate 686CBFDE00000015EFB1
  <removed>
  quit
 certificate ca 6A6967B3000000000003
  <removed>
  quit
crypto pki certificate chain CISCO_IDEVID_SUDI0
 certificate ca 5FF87B282B54DC8D42A315B568C9ADFF
  <removed>
  quit
crypto pki certificate chain TP-self-signed-145264
 certificate self-signed 01
  <removed>
  quit
```

```
power redundancy-mode redundant
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
redundancy
 mode rpr
!
vlan internal allocation policy ascending
!
vlan 11
 name POS
!
vlan 12
 name DATA
!
vlan 13
 name VOICE
!
vlan 14
 name WIRELESS
!
vlan 15
 name WIRELESS-POS
!
vlan 16
 name PARTNER
!
vlan 17
 name WIRELESS-GUEST
!
vlan 18
 name WIRELESS-CONTROL
!
vlan 19
 name WAAS
!
vlan 20
 name SECURITY-SYSTEMS
!
vlan 101
 name RouterLink101
!
vlan 102
 name RouterLink102
!
vlan 1000
 name MANAGEMENT
!
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet1
 ip vrf forwarding Mgmt-vrf
 no ip address
 shutdown
 speed auto
 duplex auto
!
interface TenGigabitEthernet3/1
 shutdown
!
interface TenGigabitEthernet3/2
 shutdown
!
interface TenGigabitEthernet3/3
 shutdown
!
interface TenGigabitEthernet3/4
 shutdown
!
interface GigabitEthernet5/1
 shutdown
!
interface GigabitEthernet5/2
 shutdown
!
interface GigabitEthernet5/3
 shutdown
!
interface GigabitEthernet5/4
 shutdown
!
interface GigabitEthernet5/5
 shutdown
!
interface GigabitEthernet5/6
 shutdown
!
interface GigabitEthernet5/7
 shutdown
!
interface GigabitEthernet5/8
 shutdown
!
interface GigabitEthernet5/9
 shutdown
!
interface GigabitEthernet5/10
 shutdown
!
interface GigabitEthernet5/11
 shutdown
!
interface GigabitEthernet5/12
 shutdown
!
interface GigabitEthernet5/13
 shutdown
!
interface GigabitEthernet5/14
 shutdown
!
interface GigabitEthernet5/15
 shutdown
!
interface GigabitEthernet5/16
 shutdown
!
interface GigabitEthernet5/17
```

```
 shutdown
!
interface GigabitEthernet5/18
 shutdown
!
interface GigabitEthernet5/19
 shutdown
!
interface GigabitEthernet5/20
 shutdown
!
interface GigabitEthernet5/21
 shutdown
!
interface GigabitEthernet5/22
 shutdown
!
interface GigabitEthernet5/23
 shutdown
!
interface GigabitEthernet5/24
 shutdown
!
interface GigabitEthernet5/25
 shutdown
!
interface GigabitEthernet5/26
 shutdown
!
interface GigabitEthernet5/27
 shutdown
!
interface GigabitEthernet5/28
 shutdown
!
interface GigabitEthernet5/29
 shutdown
!
interface GigabitEthernet5/30
 shutdown
!
interface GigabitEthernet5/31
 shutdown
!
interface GigabitEthernet5/32
 shutdown
!
interface GigabitEthernet5/33
 shutdown
!
interface GigabitEthernet5/34
 shutdown
!
interface GigabitEthernet5/35
 shutdown
!
interface GigabitEthernet5/36
 shutdown
!
interface GigabitEthernet5/37
 shutdown
!
interface GigabitEthernet5/38
 shutdown
```

```
!
interface GigabitEthernet5/39
 shutdown
!
interface GigabitEthernet5/40
 shutdown
!
interface GigabitEthernet5/41
 shutdown
!
interface GigabitEthernet5/42
 shutdown
!
interface GigabitEthernet5/43
 shutdown
!
interface GigabitEthernet5/44
 shutdown
!
interface GigabitEthernet5/45
 shutdown
!
interface GigabitEthernet5/46
 shutdown
!
interface GigabitEthernet5/47
 shutdown
!
interface GigabitEthernet5/48
 shutdown
!
interface GigabitEthernet6/1
!
interface GigabitEthernet6/2
 shutdown
!
interface GigabitEthernet6/3
 shutdown
!
interface GigabitEthernet6/4
 shutdown
!
interface GigabitEthernet6/5
 shutdown
!
interface GigabitEthernet6/6
 shutdown
!
interface GigabitEthernet6/7
 shutdown
!
interface GigabitEthernet6/8
 shutdown
!
interface GigabitEthernet6/9
 shutdown
!
interface GigabitEthernet6/10
 description MSP-A2-LRG-1
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet6/11
```

```
 shutdown
!
interface GigabitEthernet6/12
 shutdown
!
interface GigabitEthernet6/13
 shutdown
!
interface GigabitEthernet6/14
 shutdown
!
interface GigabitEthernet6/15
 shutdown
!
interface GigabitEthernet6/16
 shutdown
!
interface GigabitEthernet6/17
 description WLC-A2-LRG-1_G1
 switchport access vlan 18
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet6/18
 description WLC-A2-LRG-1_G2
 switchport trunk allowed vlan 14-17
 switchport mode trunk
!
interface GigabitEthernet6/19
 shutdown
!
interface GigabitEthernet6/20
 shutdown
!
interface GigabitEthernet6/21
 shutdown
!
interface GigabitEthernet6/22
 shutdown
!
interface GigabitEthernet6/23
 shutdown
!
interface GigabitEthernet6/24
 shutdown
!
interface GigabitEthernet6/25
 shutdown
!
interface GigabitEthernet6/26
 shutdown
!
interface GigabitEthernet6/27
 shutdown
!
interface GigabitEthernet6/28
 shutdown
!
interface GigabitEthernet6/29
 shutdown
!
interface GigabitEthernet6/30
 shutdown
!
```

```
interface GigabitEthernet6/31
 shutdown
!
interface GigabitEthernet6/32
 shutdown
!
interface GigabitEthernet6/33
 shutdown
!
interface GigabitEthernet6/34
 shutdown
!
interface GigabitEthernet6/35
 shutdown
!
interface GigabitEthernet6/36
 shutdown
!
interface GigabitEthernet6/37
 shutdown
!
interface GigabitEthernet6/38
 shutdown
!
interface GigabitEthernet6/39
 shutdown
!
interface GigabitEthernet6/40
 shutdown
!
interface GigabitEthernet6/41
 switchport mode trunk
!
interface GigabitEthernet6/42
 shutdown
!
interface GigabitEthernet6/43
 switchport mode trunk
!
interface GigabitEthernet6/44
 shutdown
!
interface GigabitEthernet6/45
 switchport mode trunk
!
interface GigabitEthernet6/46
!
interface GigabitEthernet6/47
 switchport mode trunk
!
interface GigabitEthernet6/48
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.111.11 255.255.255.0
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.10.111.1
no ip http server
```

```
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
!
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
no snmp-server enable traps license
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps errdisable
snmp-server enable traps vlan-membership
snmp-server enable traps mac-notification change move threshold
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
banner exec ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
```

```
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^CC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 17202862
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end

S-A2-LRG-1#
```

S-A2-Lrg-2

```
S-A2-LRG-2#sh run
Building configuration...
```

```
Current configuration : 20118 bytes
!
! Last configuration change at 02:45:12 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:45:13 PSTDST Sat Apr 30 2011 by retail
!
version 15.0
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service compress-config
service sequence-numbers
!
hostname S-A2-LRG-2
!
boot-start-marker
boot system flash bootflash:cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
boot-end-marker
!
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
ip subnet-zero
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
!
no ip bootp server
ip vrf Mgmt-vrf
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
vtp mode transparent
!
password encryption aes
```

```
!
crypto pki trustpoint CISCO_IDEVID_SUDI
 revocation-check none
 rsakeypair CISCO_IDEVID_SUDI
!
crypto pki trustpoint CISCO_IDEVID_SUDI0
 revocation-check none
!
crypto pki trustpoint TP-self-signed-145261
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-145261
 revocation-check none
 rsakeypair TP-self-signed-145261
!
!
crypto pki certificate chain CISCO_IDEVID_SUDI
 certificate 6B46CD9B00000015F50E
  <removed>
  quit
 certificate ca 6A6967B3000000000003
  <removed>
  quit
crypto pki certificate chain CISCO_IDEVID_SUDI0
 certificate ca 5FF87B282B54DC8D42A315B568C9ADFF
  <removed>
  quit
crypto pki certificate chain TP-self-signed-145261
 certificate self-signed 01
  <removed>
  quit
power redundancy-mode redundant
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
redundancy
 mode rpr
!
vlan internal allocation policy ascending
!
vlan 11
 name POS
!
vlan 12
 name DATA
!
vlan 13
 name VOICE
!
vlan 14
 name WIRELESS
!
vlan 15
 name WIRELESS-POS
!
vlan 16
 name PARTNER
```

```
!
vlan 17
 name WIRELESS-GUEST
!
vlan 18
 name WIRELESS-CONTROL
!
vlan 19
 name WAAS
!
vlan 20
 name SECURITY-SYSTEMS
!
vlan 101
 name RouterLink101
!
vlan 102
 name RouterLink102
!
vlan 1000
 name MANAGEMENT
!
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet1
 ip vrf forwarding Mgmt-vrf
 no ip address
 shutdown
 speed auto
 duplex auto
!
interface TenGigabitEthernet3/1
 shutdown
!
interface TenGigabitEthernet3/2
 shutdown
!
interface TenGigabitEthernet3/3
 shutdown
!
interface TenGigabitEthernet3/4
 shutdown
!
interface GigabitEthernet6/1
!
interface GigabitEthernet6/2
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/3
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/4
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/5
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/6
```

```
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/7
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/10
 description MSP-A2-LRG-1
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet6/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/13
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/14
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/15
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/16
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/19
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/21
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet6/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/23
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/24
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/26
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/28
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/29
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/30
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/31
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/32
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/33
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/34
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/35
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/36
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/37
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet6/38
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/39
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/40
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/41
 switchport mode trunk
!
interface GigabitEthernet6/42
!
interface GigabitEthernet6/43
 switchport mode trunk
!
interface GigabitEthernet6/44
!
interface GigabitEthernet6/45
 switchport mode trunk
!
interface GigabitEthernet6/46
!
interface GigabitEthernet6/47
 switchport mode trunk
!
interface GigabitEthernet6/48
!
interface Vlan1
 no ip address
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.111.12 255.255.255.0
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.10.111.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
!
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
```

```
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
no snmp-server enable traps license
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps errdisable
snmp-server enable traps vlan-membership
snmp-server enable traps mac-notification change move threshold
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
banner exec ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^CC
WARNING:
```

```
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 17211501
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

S-A2-Lrg-3

```
S-A2-LRG-3#sh run
Building configuration...

Current configuration : 20730 bytes
!
! Last configuration change at 02:52:21 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:52:23 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname S-A2-LRG-3
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
logging monitor informational
enable secret 5 <removed>
!
```

```
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
macro name dot1x
switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
@
!
macro global description dot1x
macro auto sticky
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authentication dot1x default group radius local
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa authorization configuration default group radius
aaa accounting update newinfo
aaa accounting auth-proxy default start-stop group radius
aaa accounting dot1x default start-stop group radius
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
aaa server radius dynamic-author
 client 192.168.42.111
 server-key 7 <removed>
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
authentication mac-move permit
!
!
ip dhcp snooping vlan 1,11
no ip dhcp snooping information option
```

```
ip dhcp snooping
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
ip device tracking
ip admission name ise proxy http inactivity-time 60
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
vtp mode transparent
!
cts sxp enable
cts sxp default source-ip 10.10.111.13
password encryption aes
!
crypto pki trustpoint TP-self-signed-4268543232
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4268543232
 revocation-check none
 rsakeypair TP-self-signed-4268543232
!
!
crypto pki certificate chain TP-self-signed-4268543232
 certificate self-signed 01
  <removed>
  quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
dot1x system-auth-control
!
fallback profile ise
 ip access-group ACL-DEFAULT in
 ip admission ise
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
vlan 11
 name POS
!
vlan 12
 name DATA
!
vlan 13
 name VOICE
!
vlan 14
 name WIRELESS
!
vlan 15
 name WIRELESS-POS
!
vlan 16
 name PARTNER
!
vlan 17
```

```
 name WIRELESS-GUEST
!
vlan 18
 name WIRELESS-CONTROL
!
vlan 19
 name WAAS
!
vlan 20
 name SECURITY-SYSTEMS
!
vlan 101
 name RouterLink101
!
vlan 102
 name RouterLink102
!
vlan 1000
 name MANAGEMENT
!
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 description uplink
!
interface GigabitEthernet0/2
 description uplink
!
interface GigabitEthernet0/3
 shutdown
!
interface GigabitEthernet0/4
 description Cisco9971 IP phone
 switchport access vlan 11
 switchport voice vlan 13
 spanning-tree portfast
!
interface GigabitEthernet0/5
 description IP Camera - 4300
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/6
 description CIAC-GW
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/7
 shutdown
!
interface GigabitEthernet0/8
 shutdown
!
interface GigabitEthernet0/9
 shutdown
!
interface GigabitEthernet0/10
 shutdown
```

```
!
interface GigabitEthernet0/11
 shutdown
!
interface GigabitEthernet0/12
 shutdown
!
interface GigabitEthernet0/13
 shutdown
!
interface GigabitEthernet0/14
 shutdown
!
interface GigabitEthernet0/15
 shutdown
!
interface GigabitEthernet0/16
 shutdown
!
interface GigabitEthernet0/17
 shutdown
!
interface GigabitEthernet0/18
 shutdown
!
interface GigabitEthernet0/19
 shutdown
!
interface GigabitEthernet0/20
 shutdown
!
interface GigabitEthernet0/21
 shutdown
!
interface GigabitEthernet0/22
 shutdown
!
interface GigabitEthernet0/23
 shutdown
!
interface GigabitEthernet0/24
 shutdown
!
interface GigabitEthernet0/25
 description open-mode 802.1x+mab+mda+acl
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/26
 description mobile worker
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/27
 shutdown
!
interface GigabitEthernet0/28
 shutdown
!
interface GigabitEthernet0/29
 shutdown
!
interface GigabitEthernet0/30
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
```

```
interface GigabitEthernet0/31
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/32
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/33
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/34
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/35
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/36
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/37
 shutdown
!
interface GigabitEthernet0/38
 shutdown
!
interface GigabitEthernet0/39
 shutdown
!
interface GigabitEthernet0/40
 shutdown
!
interface GigabitEthernet0/41
 shutdown
!
interface GigabitEthernet0/42
 shutdown
!
interface GigabitEthernet0/43
 shutdown
!
interface GigabitEthernet0/44
 shutdown
!
interface GigabitEthernet0/45
 shutdown
!
interface GigabitEthernet0/46
 shutdown
!
interface GigabitEthernet0/47
 shutdown
!
interface GigabitEthernet0/48
 shutdown
!
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
```

```
interface GigabitEthernet1/3
 shutdown
!
interface GigabitEthernet1/4
 shutdown
!
interface TenGigabitEthernet1/1
 shutdown
!
interface TenGigabitEthernet1/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.111.13 255.255.255.0
!
ip default-gateway 10.10.111.1
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
ip access-list extended ACL-ALLOW
 permit ip any any
ip access-list extended ACL-DEFAULT
 remark DHCP
 permit udp any eq bootpc any eq bootps
 remark DNS
 permit udp any any eq domain
 remark ICMP Ping
 permit icmp any any
 remark PXE Boot
 permit udp any any eq tftp
 remark URL Redirect
 permit tcp any host 192.168.42.111 eq www
 permit tcp any host 192.168.42.111 eq 443
 permit tcp any host 192.168.42.112 eq www
 permit tcp any host 192.168.42.112 eq 443
 remark Guest Portal
 permit tcp any host 192.168.42.111 eq 8443
 permit tcp any host 192.168.42.112 eq 8443
 deny   ip any any
ip access-list extended ACL-POSTURE-REDIRECT
 deny   ip any host 192.168.42.111
 deny   ip any host 192.168.42.130
 permit ip any any
ip access-list extended ACL-WEBAUTH-REDIRECT
 remark Don't match traffic sent to ISE PDP Nodes
 deny   ip any host 192.168.42.111
 deny   ip any host 192.168.42.112
 deny   ip any host 10.35.48.242
 deny   ip any host 171.71.169.207
 permit ip any any
!
ip sla enable reaction-alerts
```

```
logging trap debugging
logging origin-id ip
logging source-interface Vlan1000
logging 192.168.42.124
logging host 192.168.42.111 transport udp port 20514
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
snmp-server host 192.168.42.111 version 2c retaillabISE  dot1x mac-notification snmp
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 5 tries 3
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
radius-server vsa send accounting
radius-server vsa send authentication
!
banner exec ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^CC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36027134
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
mac address-table notification change interval 0
mac address-table notification change
end
```

S-A2-Lrg-4

```
S-A2-LRG-4#sh run
Building configuration...

Current configuration : 26605 bytes
!
! Last configuration change at 02:56:42 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:56:45 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname S-A2-LRG-4
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed> username emc-ncm privilege 15 secret 5
<removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
macro auto device media-player ACCESS_VLAN=12
macro auto device ip-camera ACCESS_VLAN=20
macro auto device phone ACCESS_VLAN=17 VOICE_VLAN=13
macro auto device access-point ACCESS_VLAN=18
macro auto device lightweight-ap ACCESS_VLAN=18
!
macro auto global processing fallback cdp
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authentication dot1x default group radius local
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting update newinfo
aaa accounting dot1x default start-stop group radius
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
authentication mac-move permit
```

```
ip subnet-zero
no ip source-route
!
!
ip domain-name cisco-irn.com
ip host nac-2 192.168.42.112
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
mls qos map policed-dscp  24 26 46 to 0
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
password encryption aes
!
crypto pki trustpoint TP-self-signed-4268542976
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4268542976
 revocation-check none
 rsakeypair TP-self-signed-4268542976
```

```
!
!
crypto pki certificate chain TP-self-signed-4268542976
 certificate self-signed 01
  <removed> 1
  quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
dot1x system-auth-control
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map match-all AutoQoS-VoIP-RTP-Trust
 match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
 match ip dscp cs3  af31
!
!
policy-map AutoQoS-Police-CiscoPhone
 class AutoQoS-VoIP-RTP-Trust
  set dscp ef
  police 320000 8000 exceed-action policed-dscp-transmit
 class AutoQoS-VoIP-Control-Trust
  set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
!
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 macro description CISCO_SWITCH_EVENT
 auto qos voip trust
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 macro description CISCO_SWITCH_EVENT
 auto qos voip trust
!
interface GigabitEthernet0/3
 description AIR-CAP3502E
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode access
 switchport block unicast
 switchport port-security aging time 1
 switchport port-security violation protect
 switchport port-security aging type inactivity
 load-interval 30
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust dscp
 macro description CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 15
!
interface GigabitEthernet0/4
 description AIR-CAP3502I
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode access
 switchport block unicast
 switchport port-security aging time 1
 switchport port-security violation protect
 switchport port-security aging type inactivity
 load-interval 30
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust dscp
 macro description CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 15
!
interface GigabitEthernet0/5
 shutdown
!
interface GigabitEthernet0/6
 shutdown
!
interface GigabitEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 macro description CISCO_SWITCH_EVENT
 auto qos voip trust
!
interface GigabitEthernet0/8
 shutdown
```

```
!
interface GigabitEthernet0/9
 shutdown
!
interface GigabitEthernet0/10
 shutdown
!
interface GigabitEthernet0/11
 description Cisco7975 IP phone
 switchport mode access
 switchport block unicast
 switchport voice vlan 2
 switchport port-security maximum 3
 switchport port-security maximum 2 vlan access
 switchport port-security
 switchport port-security aging time 1
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 load-interval 30
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description CISCO_PHONE_EVENT
 auto qos voip cisco-phone
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AutoQoS-Police-CiscoPhone
 ip dhcp snooping limit rate 15
!
interface GigabitEthernet0/12
 shutdown
!
interface GigabitEthernet0/13
 shutdown
!
interface GigabitEthernet0/14
 shutdown
!
interface GigabitEthernet0/15
 shutdown
!
interface GigabitEthernet0/16
 shutdown
!
interface GigabitEthernet0/17
 shutdown
!
interface GigabitEthernet0/18
 shutdown
!
interface GigabitEthernet0/19
 shutdown
!
interface GigabitEthernet0/20
 shutdown
!
interface GigabitEthernet0/21
 shutdown
!
```

```
interface GigabitEthernet0/22
 shutdown
!
interface GigabitEthernet0/23
 shutdown
!
interface GigabitEthernet0/24
 shutdown
!
interface GigabitEthernet0/25
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/26
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/27
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/28
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
```

```
!
interface GigabitEthernet0/29
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/30
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/31
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/32
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/33
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/34
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/35
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/36
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/37
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/38
```

```
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/39
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/40
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/41
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/42
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/43
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/44
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/45
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/46
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/47
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/48
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
interface GigabitEthernet1/3
 shutdown
!
interface GigabitEthernet1/4
 shutdown
!
interface TenGigabitEthernet1/1
 shutdown
!
interface TenGigabitEthernet1/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.111.14 255.255.255.0
!
ip default-gateway 10.10.111.1
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
ip access-list extended ACL-DEFAULT
 remark DHCP
 permit udp any eq bootpc any eq bootps
 remark DNS
 permit udp any any eq domain
 remark ICMP Ping
 permit icmp any any
 remark PXE Boot
 permit udp any any eq tftp
 remark URL Redirect
 permit tcp any host 192.168.42.111 eq www
 permit tcp any host 192.168.42.111 eq 443
 permit tcp any host 192.168.42.112 eq www
 permit tcp any host 192.168.42.112 eq 443
 remark Guest Portal
 permit tcp any host 192.168.42.111 eq 8443
 permit tcp any host 192.168.42.112 eq 8443
 deny   ip any any
ip access-list extended ACL-WEBAUTH-REDIRECT
 remark Don't match traffic sent to ISE PDP Nodes
 deny   ip any host 192.168.42.111
 deny   ip any host 192.168.42.112
 deny   ip any host 10.35.48.242
 remark Don't match traffic sent to remediation services (wwwin-download.cisco.com)
 deny   ip any host 171.71.169.207
 remark Match all other traffic for redirection
 permit ip any any
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
```

```
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
snmp-server host 192.168.42.111 version 2c retaillabISE  dot1x mac-notification snmp
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server dead-criteria time 5 tries 3
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36027569
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

S-A2-Lrg-5

```
S-A2-LRG-5#sh run
Building configuration...

Current configuration : 10739 bytes
!
! Last configuration change at 03:00:15 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 03:00:17 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname S-A2-LRG-5
!
boot-start-marker
boot-end-marker
!
shell trigger POS-Systems POS-Systems
logging buffered 51200
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
macro global description cisco-desktop
macro auto execute CISCO_LAST_RESORT_EVENT builtin CISCO_AP_AUTO_SMARTPORT ACCESS_VLAN=17
macro auto execute Retail-POS builtin CISCO_PHONE_AUTO_SMARTPORT ACCESS_VLAN=11
VOICE_VLAN=13
macro auto execute POS-Systems remote scp://SMARTPORT@192.168.42.122/POS-Systems.txt
ACCESS_VLAN=11 VOICE_VLAN=13
!
macro auto mac-address-group Retail-POS
 oui list 001C26
 oui list 001C25
 mac-address list 0021.5C02.1DEF
 mac-address list 001C.25BE.99C2
macro auto device media-player ACCESS_VLAN=12
macro auto device ip-camera ACCESS_VLAN=20
macro auto device phone ACCESS_VLAN=17 VOICE_VLAN=13
macro auto device access-point ACCESS_VLAN=18
macro auto device lightweight-ap ACCESS_VLAN=18
!
macro auto global processing fallback cdp
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
password encryption aes
!
crypto pki trustpoint TP-self-signed-3964801920
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3964801920
 revocation-check none
 rsakeypair TP-self-signed-3964801920
!
!
crypto pki certificate chain TP-self-signed-3964801920
 certificate self-signed 01
  <removed>
  quit
spanning-tree mode pvst
spanning-tree extend system-id
auto qos srnd4
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh version 2
ip scp server enable
!
!
interface GigabitEthernet0/1
 switchport access vlan 17
!
interface GigabitEthernet0/2
 switchport access vlan 17
!
interface GigabitEthernet0/3
 switchport access vlan 17
!
interface GigabitEthernet0/4
 switchport access vlan 17
!
interface GigabitEthernet0/5
 switchport access vlan 17
!
interface GigabitEthernet0/6
 switchport access vlan 17
!
interface GigabitEthernet0/7
 switchport access vlan 17
!
interface GigabitEthernet0/8
 switchport access vlan 17
!
interface GigabitEthernet0/9
 description Uplink to S-A2-LRG-4 G0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 1 30 35 5
 queue-set 2
 priority-queue out
 mls qos trust cos
 macro description CISCO_SWITCH_EVENT
 auto qos trust
!
interface GigabitEthernet0/10
!
interface Vlan1
 no ip address
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.111.15 255.255.255.0
!
```

```
ip default-gateway 10.10.111.1
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131 timeout 5
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
```

```
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 speed 115200
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 22518292
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
end
```

S-a2-med-1

```
S-A2-MED-1/2#sh run
Building configuration...

Current configuration : 16629 bytes
!
! Last configuration change at 02:28:28 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:28:32 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
```

```
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname S-A2-MED-1/2
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
switch 1 provision ws-c3750x-48p
switch 2 provision ws-c3750x-48p
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
no ip source-route
no ip gratuitous-arps
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-4271428864
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4271428864
 revocation-check none
 rsakeypair TP-self-signed-4271428864
!
!
crypto pki certificate chain TP-self-signed-4271428864
```

```
 certificate self-signed 01
  <removed>  quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 10
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 description Cisco9971 IP phone
 switchport access vlan 11
 switchport trunk encapsulation dot1q
 switchport voice vlan 13
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 description Cisco7975 IP phone
 switchport access vlan 11
 switchport trunk encapsulation dot1q
 switchport voice vlan 13
 spanning-tree portfast
!
interface GigabitEthernet1/0/5
 switchport access vlan 20
!
interface GigabitEthernet1/0/6
 description CPAM Gateway
 switchport access vlan 20
!
interface GigabitEthernet1/0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/8
 switchport access vlan 17
 shutdown
!
```

```
interface GigabitEthernet1/0/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/10
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/13
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/14
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/15
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/16
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/19
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/21
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/23
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/24
 switchport access vlan 17
 shutdown
!
```

```
interface GigabitEthernet1/0/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/26
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/28
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/29
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/30
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/31
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/32
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/33
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/34
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/35
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/36
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/37
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/38
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/39
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/40
 switchport access vlan 17
 shutdown
!
```

```
interface GigabitEthernet1/0/41
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/42
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/43
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/44
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/45
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/46
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/47
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/48
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/1/1
 shutdown
!
interface GigabitEthernet1/1/2
 shutdown
!
interface GigabitEthernet1/1/3
 shutdown
!
interface GigabitEthernet1/1/4
 shutdown
!
interface TenGigabitEthernet1/1/1
 shutdown
!
interface TenGigabitEthernet1/1/2
 shutdown
!
interface GigabitEthernet2/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/3
!
interface GigabitEthernet2/0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

```
interface GigabitEthernet2/0/5
 description AIR-CAP3502E
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface GigabitEthernet2/0/6
 description AIR-LAP1262N
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface GigabitEthernet2/0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/10
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/13
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/14
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/15
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/16
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/19
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/21
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/23
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/24
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/26
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/28
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/29
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/30
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/31
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/32
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/33
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/34
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/35
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/36
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/37
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/38
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/39
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/40
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/41
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/42
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/43
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/44
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/45
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/46
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/47
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/48
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/1/1
 shutdown
!
interface GigabitEthernet2/1/2
 shutdown
!
interface GigabitEthernet2/1/3
 shutdown
!
interface GigabitEthernet2/1/4
```

```
 shutdown
!
interface TenGigabitEthernet2/1/1
 shutdown
!
interface TenGigabitEthernet2/1/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.127.11 255.255.255.0
!
ip default-gateway 10.10.127.1
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
```

```
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 speed 115200
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
scheduler interval 500
ntp clock-period 36027426
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end

S-A2-MED-1/2#
```

S-A2-Med-3

```
S-A2-MED-3#sh run
Building configuration...

Current configuration : 8650 bytes
!
! Last configuration change at 02:34:20 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:34:21 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname S-A2-MED-3
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
no ip source-route
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-1308417408
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1308417408
 revocation-check none
 rsakeypair TP-self-signed-1308417408
!
!
crypto pki certificate chain TP-self-signed-1308417408
 certificate self-signed 01
  <removed>  quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet0/1
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/2
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/3
 switchport access vlan 17
 shutdown
```

```
!
interface FastEthernet0/4
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/7
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.127.13 255.255.255.0
!
ip default-gateway 10.10.127.1
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
```

```
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                     **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    *                     **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO ADMINISTRATOR OR OTHEMIME WITHOUT
FU L
NFORCEMENT OFFCIAL NDPRSETHO OF STATEAND FEER^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 speed 115200
line vty 0 4
```

```
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36028775
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

S-A2-Mini-1

```
S-A2-Mini-1#sh run
Building configuration...

Current configuration : 9017 bytes
!
! Last configuration change at 02:15:02 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:15:04 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname S-A2-Mini-1
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
ip subnet-zero
no ip source-route
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-1919348736
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1919348736
 revocation-check none
 rsakeypair TP-self-signed-1919348736
!
!
crypto pki certificate chain TP-self-signed-1919348736
 certificate self-signed 01
  <removed>
  quit
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport access vlan 17
 shutdown
!
```

```
interface GigabitEthernet0/3
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/4
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/5
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/6
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/7
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/8
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.159.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.159.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
control-plane
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
```

```
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36028654
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

S-A2-Mini-2

```
S-A2-Mini-2#sh run
Building configuration...

Current configuration : 9094 bytes
!
! Last configuration change at 02:19:10 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:19:11 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname S-A2-Mini-2
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
ip subnet-zero
no ip source-route
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-1919334912
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1919334912
 revocation-check none
 rsakeypair TP-self-signed-1919334912
!
!
crypto pki certificate chain TP-self-signed-1919334912
 certificate self-signed 01
  <removed>
  quit
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
!
```

```
interface GigabitEthernet0/1
 description AIR-CAP3502E
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/3
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/4
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/5
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/6
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/7
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/8
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.159.12 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.159.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
```

```
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
control-plane
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
```

```
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36028680
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

S-A2-MSP-1

```
Building configuration...

Current configuration : 10554 bytes
!
! Last configuration change at 02:08:19 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:08:21 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname S-A2-MSP-1
!
logging buffered 50000 debugging
```

```
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
ip subnet-zero
no ip source-route
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-4189032704
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4189032704
 revocation-check none
 rsakeypair TP-self-signed-4189032704
!
!
crypto pki certificate chain TP-self-signed-4189032704
 certificate self-signed 01
  <removed>
  quit
!
!
archive
 log config
  logging enable
  hidekeys
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
 description AIR-CAP3502I
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface GigabitEthernet0/3
!
interface GigabitEthernet0/4
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/5
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/6
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/7
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/10
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/13
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/14
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/15
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/16
 switchport access vlan 17
 shutdown
!
```

```
interface GigabitEthernet0/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/19
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/21
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/23
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/24
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/26
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/28
 switchport access vlan 17
 shutdown
!
interface TenGigabitEthernet0/1
 shutdown
!
interface TenGigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.191.11 255.255.255.0
!
ip default-gateway 10.10.191.1
ip classless
```

```
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
!
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access 88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps power-ethernet group 1
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server source-ports 1645-1646
!
control-plane
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
```

```
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36026372
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

S-A2-Small

```
S-A2-Small-1#sh run
Building configuration...

Current configuration : 16143 bytes
!
! Last configuration change at 02:23:14 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:23:18 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname S-A2-Small-1
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed> username emc-ncm privilege 15 secret 5
<removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
switch 1 provision ws-c2960s-48fps-l
switch 2 provision ws-c2960s-48fps-l
authentication mac-move permit
ip subnet-zero
no ip source-route
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
```

```
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-1383908352
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1383908352
 revocation-check none
 rsakeypair TP-self-signed-1383908352
!
!
crypto pki certificate chain TP-self-signed-1383908352
 certificate self-signed 01
  30820252 308201BB A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31333833 39303833 3532301E 170D3131 30343232 30333331
  35375A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 33383339
  30383335 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100BD50 C6915FE3 A1789C0E 11A0BABD EC2528DB 3F8FBCF6 64D90C72 AD2D2A13
  A012AB72 F5F9EEDE 4E77EDA9 D3CE6985 BA2246A1 21FF6D61 B8FFC558 331CD608
  DB59F546 838396C6 29266AF9 6B968127 75A7CE55 6D0B3734 0454EA42 24E9C995
  1AC5D0C3 0850D703 F58A2E82 6FB13D8D 372F03D8 A5B2B577 CDB7A9D5 7AFC40B6
  B26B0203 010001A3 7A307830 0F060355 1D130101 FF040530 030101FF 30250603
  551D1104 1E301C82 1A532D41 322D536D 616C6C2D 312E6369 73636F2D 69726E2E
  636F6D30 1F060355 1D230418 30168014 107F4DD8 762989FE 887F813D 62A1D871
  C9A4D3D4 301D0603 551D0E04 16041410 7F4DD876 2989FE88 7F813D62 A1D871C9
  A4D3D430 0D06092A 864886F7 0D010104 05000381 810045BF 884709EE FA837D06
  262E65C8 865912B1 44D5DE7F 459A7DEF DAEB3D94 B2D5A978 5CCF425E 1FED41CE
  2046BA9D 130DE1BD 4A7F3F99 B6AD32CA 3857A088 01083AAB 24557476 73F8AAC6
  634964A5 455F4DB2 AC36D64E EA2C71AD 296D82B6 CE1EDCCB 0724DB5D 0D332C10
  A17D5B1F E8926DC9 137519A1 521C9155 AF9AF52B 00BD
  quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 description IP Cameras - 4300
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet1/0/4
 description CPAM Gateway
 switchport access vlan 20
!
interface GigabitEthernet1/0/5
 switchport mode trunk
!
interface GigabitEthernet1/0/6
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/7
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/10
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/13
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/14
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/15
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/16
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/19
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet1/0/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/21
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/23
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/24
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/26
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/28
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/29
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/30
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/31
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/32
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/33
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/34
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/35
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet1/0/36
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/37
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/38
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/39
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/40
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/41
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/42
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/43
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/44
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/45
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/46
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/47
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/48
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/49
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/50
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/51
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet1/0/52
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/1
 shutdown
!
interface GigabitEthernet2/0/2
 shutdown
!
interface GigabitEthernet2/0/3
 description Cisco7975 IP phone
 switchport access vlan 11
 switchport voice vlan 13
 spanning-tree portfast
!
interface GigabitEthernet2/0/4
 description AIR-CAP3502I
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface GigabitEthernet2/0/5
 description Cisco9971 IP phone
 switchport access vlan 11
 switchport voice vlan 13
 spanning-tree portfast
!
interface GigabitEthernet2/0/6
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/7
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/10
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/13
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/14
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet2/0/15
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/16
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/19
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/21
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/23
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/24
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/26
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/28
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/29
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/30
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet2/0/31
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/32
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/33
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/34
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/35
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/36
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/37
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/38
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/39
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/40
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/41
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/42
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/43
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/44
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/45
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/46
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet2/0/47
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/48
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/49
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/50
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/51
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/52
 switchport access vlan 17
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.143.11 255.255.255.0
!
ip default-gateway 10.10.143.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
```

```
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^CC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 22518357
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

saccess-1

```
!
! Last configuration change at 01:58:36 PSTDST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:58:36 PSTDST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service compress-config
service sequence-numbers
!
hostname SACCESS-1
!
boot-start-marker
boot-end-marker
!
logging snmp-authfail
logging buffered 51200 debugging
enable secret 5 <removed>
!
username emc-ncm privilege 15 secret 5 <removed>
username retail privilege 15 secret 5 <removed> username bart privilege 15 secret 5
<removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
ip subnet-zero
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
no ip bootp server
ip ssh version 2
ip scp server enable
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
vtp mode transparent
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-112603
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-112603
 revocation-check none
 rsakeypair TP-self-signed-112603
!
!
crypto pki certificate chain TP-self-signed-112603
 certificate self-signed 01
  <removed>
  quit
!
!
power redundancy-mode redundant
archive
 log config
  logging enable
  hidekeys
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 20,41-43
!
vlan 44
 name PhysicalSec
!
vlan 45-50,52,62
!
vlan 64
 name Databases
!
vlan 72,146,164,256,666,1000
!
interface Loopback0
 no ip address
!
interface Port-channel1
```

```
 description to Aggregation Switches
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 logging event link-status
 flowcontrol receive on
!
interface GigabitEthernet1/1
 description SRV-DC-1
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/2
 description SRV-DC-2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 41
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/3
 description SRV-DC-3
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/4
 description SRV-DC-4
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/5
 description SRV-DC-5
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/6
 description SRV-DC-6=CUAE
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/7
 description SRV-DC-7=CCM511
 switchport access vlan 45
 spanning-tree portfast
!
interface GigabitEthernet1/8
 description SRV-DC-8 - Oracle RDBMS 10g
 switchport access vlan 64
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 64
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/9
 description MSP-DC-1
 switchport access vlan 44
 switchport trunk encapsulation dot1q
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/10
 description SRV-DC-10
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/11
 description SRV-DC-11
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/12
 description SRV-DC-12
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/13
 description SRV-DC-13
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/14
 description SRV-DC-14
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/15
 description SRV-DC-15
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/16
 description SRV-DC-16
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/17
 description SRV-DC-17
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/18
 description SRV-DC-18
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/19
 description SRV-DC-19
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/20
 description SRV-DC-20
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/21
 description SRV-DC-21
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/22
 description SRV-DC-22
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/23
 description SRV-DC-23
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/24
 description SRV-DC-24
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/25
 description SRV-DC-25
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/26
 description server 14 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/27
 description server 15 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/28
 description server 16 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/29
 description server 18 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/30
 description server 19 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/31
 description server 20 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/32
 description server 21 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/33
 description VXML Rouer VEM
 switchport access vlan 45
 spanning-tree portfast
!
interface GigabitEthernet1/34
 description SPAN to SRV-DC-28-NICE VoiceRecorder
 switchport trunk encapsulation dot1q
 spanning-tree portfast
!
interface GigabitEthernet1/35
 description Small store 1800 server e1
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 spanning-tree portfast
!
interface GigabitEthernet1/36
 description small store 1800 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/37
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/38
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/39
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/40
 description IPcelerate Server
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/41
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/42
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/43
 description EMC SAN Mgt-A
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/44
 description PRomise SAN M1
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/45
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/46
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/47
 description Uplink to RSERV-1 Management G7/1
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/48
 description Uplink to RSERV-2 Management G7/1
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast
!
interface TenGigabitEthernet1/49
 description Uplink to RAGG-1-VDC2 T1/13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 channel-group 1 mode active
 spanning-tree portfast trunk
!
interface TenGigabitEthernet1/50
 description Uplink to RAGG-2-VDC2 T1/13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 channel-group 1 mode active
 spanning-tree portfast trunk
!
interface Vlan1
 no ip address
!
interface Vlan42
 ip address 192.168.42.33 255.255.255.0
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.42.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Vlan42
!
!
logging source-interface Vlan42
logging 192.168.42.121
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
```

```
!
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access 88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan42
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
no tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server source-ports 1645-1646
!
control-plane
!
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
```

```
banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
!
monitor session 1 source interface Gi1/33
monitor session 1 destination interface Gi1/34
ntp clock-period 17181001
ntp server 192.168.0.1
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

saccess-2

```
!
! Last configuration change at 01:59:33 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:59:33 PST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service compress-config
service sequence-numbers
!
hostname SACCESS-2
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 debugging
```

```
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone PST -8
clock summer-time PST recurring
vtp mode transparent
ip subnet-zero
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
no ip bootp server
ip ssh version 2
ip scp server enable
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
power redundancy-mode redundant
!
!
!
vlan internal allocation policy ascending
!
vlan 20,40-43
!
vlan 44
 name PhysicalSec
!
vlan 45-49,52,62,64,72,146,164,256,666,1000
!
interface Port-channel2
 description to Aggregation Switches
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 logging event link-status
 flowcontrol receive on
!
interface GigabitEthernet1/1
 description SRV-DC-1
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/2
 description SRV-DC-2
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/3
 description SRV-DC-3
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/4
 description SRV-DC-4
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/5
 description SRV-DC-5
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/6
 description SRV-DC-6=CUAE
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/7
 description SRV-DC-7=CCM511
 switchport access vlan 45
 spanning-tree portfast
!
interface GigabitEthernet1/8
 description SRV-DC-8
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/9
 description MSP-DC-1
 switchport access vlan 44
 switchport trunk encapsulation dot1q
 switchport mode access
 spanning-tree portfast
```

```
!
interface GigabitEthernet1/10
 description SRV-DC-10
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/11
 description SRV-DC-11
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/12
 description SRV-DC-12
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/13
 description SRV-DC-13
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/14
 description SRV-DC-14
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/15
 description SRV-DC-15
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/16
 description SRV-DC-16
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/17
 description SRV-DC-17
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
```

```
interface GigabitEthernet1/18
 description SRV-DC-18
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/19
 description SRV-DC-19
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/20
 description SRV-DC-20
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/21
 description SRV-DC-21
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/22
 description SRV-DC-22
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/23
 description SRV-DC-23
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/24
 description SRV-DC-24
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/25
 description SRV-DC-25
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/26
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/27
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/28
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/29
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/30
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/31
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/32
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/33
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/34
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/35
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/36
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/37
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/38
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/39
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/40
```

```
 description IPcelerate Server
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/41
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/42
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/43
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/44
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/45
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/46
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 shutdown
 spanning-tree portfast trunk
!
interface GigabitEthernet1/47
 description TEMP Uplink to RSERV-1 Management G7/2
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/48
 description TEMP Uplink to RSERV-2 Management G7/2
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast
!
interface TenGigabitEthernet1/49
 description Uplink to RAGG-1-VDC2 T1/14
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 spanning-tree portfast trunk
 channel-group 2 mode active
!
interface TenGigabitEthernet1/50
 description Uplink to RAGG-2-VDC2 T1/14
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 spanning-tree portfast trunk
 channel-group 2 mode active
!
interface Vlan1
 no ip address
!
interface Vlan42
 ip address 192.168.42.34 255.255.255.0
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.42.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan42
!
!
!
logging trap debugging
logging source-interface Vlan42
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access 88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan42
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
```

```
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps flash insertion removal
snmp-server enable traps syslog
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server source-ports 1645-1646
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 17181029
ntp source Vlan42
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
end
```

SACCESS-3

```
!Command: show running-config
!Time: Sat Apr 30 01:56:18 2011

version 5.0(3)N1(1b)
feature fcoe

feature privilege
no feature telnet
no telnet server enable
feature tacacs+
cfs eth distribute
feature lacp
feature vpc
feature lldp
feature fex

username admin password 5 <removed>   role network-admin
username retail password 5 <removed>   role network-admin
username bart password 5 <removed>  role network-admin
username emc-ncm password 5 <removed>  role network-admin
enable secret 5 <removed>

banner motd #
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
#

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host SACCESS-3 192.168.41.33
tacacs-server key 7 “<removed>”
```

```
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
hostname SACCESS-3
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.41.33/32
  20 permit ip 192.168.41.101/32 192.168.41.33/32
  30 permit ip 192.168.41.102/32 192.168.41.33/32
  40 permit ip 192.168.42.111/32 192.168.41.33/32
  50 permit ip 192.168.42.122/32 192.168.41.33/32
  60 permit ip 192.168.42.131/32 192.168.41.33/32
  70 permit ip 192.168.42.133/32 192.168.41.33/32
  80 permit ip 192.168.42.138/32 192.168.41.33/32
  90 permit ip 10.19.151.99/32 192.168.41.33/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.41.33/32
  20 deny ip any any
class-map type qos class-fcoe
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
snmp-server user bart network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user admin network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user retail network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user emc-ncm network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server host 192.168.41.101 traps version 2c public  udp-port 2162
no snmp-server enable traps entity entity_mib_change
no snmp-server enable traps entity entity_module_status_change
no snmp-server enable traps entity entity_power_status_change
no snmp-server enable traps entity entity_module_inserted
no snmp-server enable traps entity entity_module_removed
no snmp-server enable traps entity entity_unrecognised_module
no snmp-server enable traps entity entity_fan_status_change
no snmp-server enable traps rf redundancy_framework
snmp-server enable traps entity fru
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
  ip route 0.0.0.0/0 192.168.41.1
vlan 1
vlan 36
  name DeviceMgmtHigh
vlan 37
  name DeviceMgmtLow
vlan 38
  name HyTrust
vlan 40
  name Server_iLO
```

```
vlan 41
  name ESX_Server
vlan 42
  name CoreManagement
vlan 43
  name WirelessSystems
vlan 45
vlan 52
  name POS
vlan 80-82,140-141
vlan 302
  fcoe vsan 2
vsan database
  vsan 2 name "Promise-2"
fcdomain fcid database
  vsan 2 wwn 21:00:00:1b:32:00:ab:0d fcid 0xee0000 area dynamic
  vsan 2 wwn 21:00:00:1b:32:00:70:0d fcid 0xee0100 area dynamic
  vsan 2 wwn 21:00:00:1b:32:00:33:0c fcid 0xee0200 area dynamic
  vsan 2 wwn 21:00:00:1b:32:00:5d:0d fcid 0xee0300 area dynamic
  vsan 2 wwn 21:00:00:1b:32:80:0b:10 fcid 0xee0400 area dynamic
  vsan 2 wwn 21:00:00:1b:32:80:52:10 fcid 0xee0500 area dynamic
  vsan 2 wwn 21:00:00:1b:32:80:da:0f fcid 0xee0600 area dynamic
  vsan 2 wwn 21:00:00:1b:32:00:3a:0c fcid 0xee0700 area dynamic
  vsan 2 wwn 21:00:00:1b:32:80:f1:0f fcid 0xee0800 area dynamic
  vsan 1 wwn 26:01:00:01:55:35:7e:44 fcid 0xee0000 dynamic
  vsan 2 wwn 21:00:00:1b:32:00:5e:0d fcid 0xee0900 area dynamic


interface port-channel3
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52

interface vfc513
  bind interface Ethernet1/13
  no shutdown

interface vfc514
  bind interface Ethernet1/14
  no shutdown

interface vfc515
  bind interface Ethernet1/15
  no shutdown

interface vfc516
  bind interface Ethernet1/16
  no shutdown

interface vfc517
  bind interface Ethernet1/17
  no shutdown

interface vfc518
  bind interface Ethernet1/18
  no shutdown

interface vfc519
  bind interface Ethernet1/19
  no shutdown

interface vfc520
  bind interface Ethernet1/20
  no shutdown
```

```
interface vfc521
  bind interface Ethernet1/21
  no shutdown

interface vfc522
  bind interface Ethernet1/22
  no shutdown

interface vfc523
  bind interface Ethernet1/23
  no shutdown

interface vfc524
  bind interface Ethernet1/24
  no shutdown

interface vfc525
  bind interface Ethernet1/25
  no shutdown

interface vfc526
  bind interface Ethernet1/26
  no shutdown

interface vfc527
  bind interface Ethernet1/27
  no shutdown

interface vfc528
  bind interface Ethernet1/28
  no shutdown

interface vfc529
  bind interface Ethernet1/29
  no shutdown

interface vfc530
  bind interface Ethernet1/30
  no shutdown

interface vfc531
  bind interface Ethernet1/31
  no shutdown

interface vfc532
  bind interface Ethernet1/32
  no shutdown

interface vfc505
  bind interface Ethernet1/5
  no shutdown

interface vfc506
  bind interface Ethernet1/6
  no shutdown

interface vfc507
  bind interface Ethernet1/7
  no shutdown

interface vfc508
  bind interface Ethernet1/8
  no shutdown
```

```
interface vfc509
  bind interface Ethernet1/9
  no shutdown

interface vfc510
  bind interface Ethernet1/10
  no shutdown

interface vfc511
  bind interface Ethernet1/11
  no shutdown

interface vfc512
  bind interface Ethernet1/12
  no shutdown
vsan database
  vsan 2 interface vfc513
  vsan 2 interface vfc514
  vsan 2 interface vfc515
  vsan 2 interface vfc516
  vsan 2 interface vfc517
  vsan 2 interface vfc518
  vsan 2 interface vfc519
  vsan 2 interface vfc520
  vsan 2 interface vfc521
  vsan 2 interface vfc522
  vsan 2 interface vfc523
  vsan 2 interface vfc524
  vsan 2 interface vfc525
  vsan 2 interface vfc526
  vsan 2 interface vfc527
  vsan 2 interface vfc528
  vsan 2 interface vfc529
  vsan 2 interface vfc530
  vsan 2 interface vfc531
  vsan 2 interface vfc532
  vsan 4094 interface vfc505
  vsan 4094 interface vfc506
  vsan 4094 interface vfc507
  vsan 4094 interface vfc508
  vsan 4094 interface vfc509
  vsan 4094 interface vfc510
  vsan 2 interface vfc511
  vsan 2 interface vfc512
  vsan 2 interface fc2/1
  vsan 2 interface fc2/2
  vsan 2 interface fc2/3
  vsan 2 interface fc2/4
  vsan 2 interface fc3/1
  vsan 2 interface fc3/2
  vsan 2 interface fc3/3
  vsan 2 interface fc3/4


interface fc2/1
  switchport description Connection to MDS-DC-1
  no shutdown

interface fc2/2

interface fc2/3

interface fc2/4
interface fc3/1
  switchport description Connection to Promise 600 san
  no shutdown

interface fc3/2

interface fc3/3

interface fc3/4

interface Ethernet1/1
  description to DC-F-UCS-1 TG0/1
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/2
  description to DC-F-UCS-1 TG0/2
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/3
  description to DC-F-UCS-2 TG0/3
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/4
  description to DC-F-UCS-2 TG0/4
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/5
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/6
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/7
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/8
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/9
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/10
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/11
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/12
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/13
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/14
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/15
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/16
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/17
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/18
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/19
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/20
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/21
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/22
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/23
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/24
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/25
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/26
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/27
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/28
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/29
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/30
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/31
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/32
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/33
  description to RAGG-1-VDC2 TG1/9
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 3 mode active

interface Ethernet1/34
  description to RAGG-1-VDC2 TG1/10
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 3 mode active

interface Ethernet1/35
  description to RAGG-2-VDC2 TG1/11
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 3 mode active

interface Ethernet1/36
  description to RAGG-2-VDC2 TG1/12
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 3 mode active

interface Ethernet1/37
  shutdown

interface Ethernet1/38
  shutdown

interface Ethernet1/39
  description to SACCESS-4
  shutdown

interface Ethernet1/40
  description to SACCESS-4
  shutdown

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4
interface Ethernet3/1

interface Ethernet3/2

interface Ethernet3/3

interface Ethernet3/4

interface mgmt0
  ip address 192.168.41.33/24
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
system default zone default-zone permit
system default zone distribute full
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
boot kickstart bootflash:/n5000-uk9-kickstart.5.0.3.N1.1b.bin
boot system bootflash:/n5000-uk9.5.0.3.N1.1b.bin
interface fc2/2
interface fc2/3
interface fc2/4
interface fc2/1
  switchport fcrxbbcredit 1
  switchport fcrxbbcredit 2 mode E
interface fc3/1
interface fc3/2
interface fc3/3
interface fc3/4
logging server 192.168.42.124 6
zone default-zone permit vsan 2
zoneset distribute full vsan 2
!Full Zone Database Section for vsan 2
zone name global_zone vsan 2
    member pwwn 26:00:00:01:55:35:7e:44
    member pwwn 26:02:00:01:55:35:7e:44
    member pwwn 10:00:00:00:c9:75:68:c3
    member pwwn 10:00:00:00:c9:77:92:e9
    member pwwn 10:00:00:00:c9:77:db:c3
    member pwwn 10:00:00:00:c9:77:dc:c3
    member pwwn 10:00:00:00:c9:77:dd:bc
    member pwwn 21:00:00:1b:32:00:33:0c
    member pwwn 21:00:00:1b:32:00:3a:0c
    member pwwn 21:00:00:1b:32:00:5d:0d
    member pwwn 21:00:00:1b:32:00:5e:0d
    member pwwn 21:00:00:1b:32:00:70:0d
    member pwwn 21:00:00:1b:32:00:ab:0d
    member pwwn 21:00:00:1b:32:80:0b:10
    member pwwn 21:00:00:1b:32:80:52:10
    member pwwn 21:00:00:1b:32:80:da:0f
    member pwwn 21:00:00:1b:32:80:f1:0f

zoneset name promise-2_zs vsan 2
    member global_zone

zoneset activate name promise-2_zs vsan 2
```

SACCESS-4

```
!Command: show running-config
!Time: Sat Apr 30 01:57:14 2011

version 5.0(3)N1(1b)
feature fcoe

feature privilege
no feature telnet
no telnet server enable
feature tacacs+
cfs eth distribute
feature lacp
feature vpc
feature lldp
feature fex

username admin password 5 <removed> role network-admin
username retail password 5 <removed> role network-admin
username emc-ncm password 5 <removed> role network-admin
username bart password 5 <removed> role network-admin
enable secret 5 <removed>

banner motd #
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
#

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host SACCESS-4 192.168.41.34
tacacs-server key 7 “<removed>”
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
switchname SACCESS-4
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.41.34/32
  20 permit ip 192.168.41.101/32 192.168.41.34/32
  30 permit ip 192.168.41.102/32 192.168.41.34/32
  40 permit ip 192.168.42.111/32 192.168.41.34/32
  50 permit ip 192.168.42.122/32 192.168.41.34/32
  60 permit ip 192.168.42.131/32 192.168.41.34/32
  70 permit ip 192.168.42.133/32 192.168.41.34/32
  80 permit ip 192.168.42.138/32 192.168.41.34/32
  90 permit ip 10.19.151.99/32 192.168.41.34/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.41.34/32
  20 deny ip any any
class-map type qos class-fcoe
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
snmp-server user bart network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user admin network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user retail network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user emc-ncm network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server enable traps entity fru
no snmp-server enable traps entity entity_mib_change
no snmp-server enable traps entity entity_module_status_change
no snmp-server enable traps entity entity_power_status_change
no snmp-server enable traps entity entity_module_inserted
no snmp-server enable traps entity entity_module_removed
no snmp-server enable traps entity entity_unrecognised_module
no snmp-server enable traps entity entity_fan_status_change
no snmp-server enable traps rf redundancy_framework
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
  ip route 0.0.0.0/0 192.168.41.1
vlan 1
vlan 36
  name DeviceMgmtHigh
vlan 37
  name DeviceMgmtLow
vlan 38
  name HyTrust
vlan 40
  name Server_iLO
vlan 41
  name ESX_Server
vlan 42
  name CoreManagement
vlan 45,80-82,141-142
vlan 402
  fcoe vsan 2
vsan database
  vsan 2
fcdomain fcid database
  vsan 2 wwn 21:01:00:1b:32:20:5e:0d fcid 0xa20000 area dynamic
  vsan 2 wwn 21:01:00:1b:32:20:ab:0d fcid 0xa20100 area dynamic
  vsan 2 wwn 21:01:00:1b:32:20:70:0d fcid 0xa20200 area dynamic
  vsan 2 wwn 21:01:00:1b:32:20:33:0c fcid 0xa20300 area dynamic
  vsan 2 wwn 21:01:00:1b:32:20:5d:0d fcid 0xa20400 area dynamic
  vsan 2 wwn 21:01:00:1b:32:a0:0b:10 fcid 0xa20500 area dynamic
  vsan 2 wwn 21:01:00:1b:32:a0:52:10 fcid 0xa20600 area dynamic
  vsan 2 wwn 21:01:00:1b:32:a0:da:0f fcid 0xa20700 area dynamic
  vsan 2 wwn 21:01:00:1b:32:a0:f1:0f fcid 0xa20800 area dynamic
  vsan 2 wwn 21:01:00:1b:32:20:3a:0c fcid 0xa20900 area dynamic


interface port-channel4
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52

interface vfc513
  bind interface Ethernet1/13
  no shutdown

interface vfc514
  bind interface Ethernet1/14
  no shutdown

interface vfc515
  bind interface Ethernet1/15
  no shutdown

interface vfc516
  bind interface Ethernet1/16
  no shutdown

interface vfc517
  bind interface Ethernet1/17
  no shutdown

interface vfc518
  bind interface Ethernet1/18
  no shutdown

interface vfc519
  bind interface Ethernet1/19
  no shutdown

interface vfc520
  bind interface Ethernet1/20
  no shutdown

interface vfc521
  bind interface Ethernet1/21
  no shutdown

interface vfc522
  bind interface Ethernet1/22
  no shutdown

interface vfc523
  bind interface Ethernet1/23
  no shutdown

interface vfc524
  bind interface Ethernet1/24
  no shutdown

interface vfc525
  bind interface Ethernet1/25
  no shutdown

interface vfc526
  bind interface Ethernet1/26
  no shutdown

interface vfc527
```

```
  bind interface Ethernet1/27
  no shutdown

interface vfc528
  bind interface Ethernet1/28
  no shutdown

interface vfc529
  bind interface Ethernet1/29
  no shutdown

interface vfc530
  bind interface Ethernet1/30
  no shutdown

interface vfc531
  bind interface Ethernet1/31
  no shutdown

interface vfc532
  bind interface Ethernet1/32
  no shutdown

interface vfc505
  bind interface Ethernet1/5
  no shutdown

interface vfc506
  bind interface Ethernet1/6
  no shutdown

interface vfc507
  bind interface Ethernet1/7
  no shutdown

interface vfc508
  bind interface Ethernet1/8
  no shutdown

interface vfc509
  bind interface Ethernet1/9
  no shutdown

interface vfc510
  bind interface Ethernet1/10
  no shutdown

interface vfc511
  bind interface Ethernet1/11
  no shutdown

interface vfc512
  bind interface Ethernet1/12
  no shutdown
vsan database
  vsan 2 interface vfc513
  vsan 2 interface vfc514
  vsan 2 interface vfc515
  vsan 2 interface vfc516
  vsan 2 interface vfc517
  vsan 2 interface vfc518
  vsan 2 interface vfc519
  vsan 2 interface vfc520
  vsan 2 interface vfc521
  vsan 2 interface vfc522
  vsan 2 interface vfc523
  vsan 2 interface vfc524
  vsan 2 interface vfc525
  vsan 2 interface vfc526
  vsan 2 interface vfc527
  vsan 2 interface vfc528
  vsan 2 interface vfc529
  vsan 2 interface vfc530
  vsan 2 interface vfc531
  vsan 2 interface vfc532
  vsan 2 interface vfc505
  vsan 2 interface vfc506
  vsan 2 interface vfc507
  vsan 2 interface vfc508
  vsan 2 interface vfc509
  vsan 2 interface vfc510
  vsan 2 interface vfc511
  vsan 2 interface vfc512
  vsan 2 interface fc3/1


interface fc2/1
  switchport description Connection to MDS-DC-1
  no shutdown

interface fc2/2

interface fc2/3

interface fc2/4

interface fc3/1
  switchport description Connection to Promise 600 san
  no shutdown

interface fc3/2

interface fc3/3

interface fc3/4

interface Ethernet1/1
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/2
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/3
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/4
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/5
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/6
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/7
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/8
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/9
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/10
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/11
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/12
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/13
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/14
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/15
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/16
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/17
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/18
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/19
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/20
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/21
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/22
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/23
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/24
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/25
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/26
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/27
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/28
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/29
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/30
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/31
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/32
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/33
  description to RAGG-2-VDC2 TG1/9
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 4 mode active

interface Ethernet1/34
  description to RAGG-2-VDC2 TG1/10
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 4 mode active

interface Ethernet1/35
  description to RAGG-1-VDC2 TG1/11
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 4 mode active

interface Ethernet1/36
```

```
  description to RAGG-1-VDC2 TG1/12
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 4 mode active

interface Ethernet1/37
  shutdown

interface Ethernet1/38
  shutdown

interface Ethernet1/39
  description link to SACCESS-3
  shutdown

interface Ethernet1/40
  description link to SACCESS-3
  shutdown

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet3/1

interface Ethernet3/2

interface Ethernet3/3

interface Ethernet3/4

interface mgmt0
  ip address 192.168.41.34/24
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
boot kickstart bootflash:/n5000-uk9-kickstart.5.0.3.N1.1b.bin
boot system bootflash:/n5000-uk9.5.0.3.N1.1b.bin
interface fc2/1
interface fc2/2
interface fc2/3
interface fc2/4
interface fc3/1
interface fc3/2
interface fc3/3
interface fc3/4
logging server 192.168.42.124 6
zone default-zone permit vsan 2
!Full Zone Database Section for vsan 2
zone name global_zone vsan 2
zoneset name promise-2_zs vsan 2
    member global_zone
```

saccess-5

```
!
! Last configuration change at 02:02:07 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 02:02:10 PST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname SACCESS-5
!
boot-start-marker
boot-end-marker
!
logging buffered 51200
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PST recurring
switch 1 provision ws-c3750e-48td
system mtu routing 1500
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 65535
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-2654502656
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2654502656
 revocation-check none
 rsakeypair TP-self-signed-2654502656
!
!
crypto pki certificate chain TP-self-signed-2654502656
 certificate self-signed 01
  <removed>   quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
vlan dot1q tag native
!
ip ssh version 2
ip scp server enable
!
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 description SRV-DC-22 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 description SRV-DC-23 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 description SRV-DC-24 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 description SRV-DC-25 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/5
 description SRV-DC-26 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/6
 description SRV-DC-27 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/7
 description SRV-DC-28 iLO
 switchport access vlan 40
 spanning-tree portfast
```

```
!
interface GigabitEthernet1/0/8
 description SRV-DC-29 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/9
 description SRV-DC-30 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/10
 description SRV-DC-31 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/11
 description DC-UCSFabric-1-A Mgmt0
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/12
 description DC-UCSFabric-1-B Mgmt0
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/13
 description DC-ASA-1 Mgmt0
 switchport access vlan 42
 spanning-tree portfast
!
interface GigabitEthernet1/0/14
 description DC-ASA-2 Mgmt0
 switchport access vlan 42
 spanning-tree portfast
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
 description SRV-DC-22 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/23
 description SRV-DC-23 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/24
 description SRV-DC-24 ESXi
 switchport access vlan 41
 spanning-tree portfast
```

```
!
interface GigabitEthernet1/0/25
 description SRV-DC-25 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/26
 description SRV-DC-26 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/27
 description SRV-DC-27 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/28
 description SRV-DC-28 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/29
 description SRV-DC-29 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/30
 description SRV-DC-30 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/31
 description SRV-DC-31 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/32
 description SRV-DC-32 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/33
 description SRV-DC-33 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/34
 description SRV-DC-34 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/35
 description SRV-DC-35 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/36
!
interface GigabitEthernet1/0/37
 description SACCESS-3 Mgmt
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/38
```

```
 description SACCESS-4 Mgmt
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/39
 description RCORE-1 Mgmt-a
 switchport access vlan 42
 spanning-tree portfast
!
interface GigabitEthernet1/0/40
 description RCORE-1 Mgmt-b
 switchport access vlan 42
 spanning-tree portfast
!
interface GigabitEthernet1/0/41
 description RCORE-2 Mgmt-a
 switchport access vlan 42
 spanning-tree portfast
!
interface GigabitEthernet1/0/42
 description RCORE-2 Mgmt-b
 switchport access vlan 42
 spanning-tree portfast
!
interface GigabitEthernet1/0/43
!
interface GigabitEthernet1/0/44
!
interface GigabitEthernet1/0/45
!
interface GigabitEthernet1/0/46
!
interface GigabitEthernet1/0/47
 description Uplink to RAGG-2-vdc2 T2/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/48
 description Uplink to RAGG-1-vdc2 T2/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
interface GigabitEthernet1/0/51
!
interface GigabitEthernet1/0/52
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan41
 ip address 192.168.41.222 255.255.255.0
!
interface Vlan42
 ip address 192.168.42.30 255.255.255.0
!
```

```
interface Vlan1000
 no ip address
!
ip default-gateway 192.168.42.1
ip classless
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan42
!
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan42
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan42
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
```

```
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131 timeout 5
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36029147
ntp source Vlan42
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
```

```
end
```

swan-1

```
!
! Last configuration change at 01:33:45 PST Sat Apr 30 2011 by retail
! NVRAM config last updated at 01:33:48 PST Sat Apr 30 2011 by retail
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname SWAN-1
!
boot-start-marker
boot-end-marker
!
logging buffered 51200
enable secret 5 <removed>
!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PST recurring
switch 1 provision ws-c3750-48p
switch 2 provision ws-c3750-48p
system mtu routing 1500
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
```

```
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-722491520
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-722491520
 revocation-check none
 rsakeypair TP-self-signed-722491520
!
!
crypto pki certificate chain TP-self-signed-722491520
 certificate self-signed 01
  <removed>   quit
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet1/0/1
!
interface FastEthernet1/0/2
!
interface FastEthernet1/0/3
!
interface FastEthernet1/0/4
!
interface FastEthernet1/0/5
!
interface FastEthernet1/0/6
!
interface FastEthernet1/0/7
!
interface FastEthernet1/0/8
!
interface FastEthernet1/0/9
!
interface FastEthernet1/0/10
!
interface FastEthernet1/0/11
!
interface FastEthernet1/0/12
!
interface FastEthernet1/0/13
!
interface FastEthernet1/0/14
!
interface FastEthernet1/0/15
!
interface FastEthernet1/0/16
!
interface FastEthernet1/0/17
!
```

```
interface FastEthernet1/0/18
!
interface FastEthernet1/0/19
!
interface FastEthernet1/0/20
!
interface FastEthernet1/0/21
!
interface FastEthernet1/0/22
!
interface FastEthernet1/0/23
!
interface FastEthernet1/0/24
!
interface FastEthernet1/0/25
!
interface FastEthernet1/0/26
!
interface FastEthernet1/0/27
!
interface FastEthernet1/0/28
!
interface FastEthernet1/0/29
!
interface FastEthernet1/0/30
!
interface FastEthernet1/0/31
!
interface FastEthernet1/0/32
!
interface FastEthernet1/0/33
!
interface FastEthernet1/0/34
!
interface FastEthernet1/0/35
!
interface FastEthernet1/0/36
!
interface FastEthernet1/0/37
!
interface FastEthernet1/0/38
!
interface FastEthernet1/0/39
!
interface FastEthernet1/0/40
!
interface FastEthernet1/0/41
!
interface FastEthernet1/0/42
!
interface FastEthernet1/0/43
!
interface FastEthernet1/0/44
!
interface FastEthernet1/0/45
!
interface FastEthernet1/0/46
!
interface FastEthernet1/0/47
!
interface FastEthernet1/0/48
 description SNiffer Uplink to Server10_fe2
!
interface GigabitEthernet1/0/1
```

```
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
!
interface FastEthernet2/0/1
!
interface FastEthernet2/0/2
!
interface FastEthernet2/0/3
!
interface FastEthernet2/0/4
!
interface FastEthernet2/0/5
!
interface FastEthernet2/0/6
!
interface FastEthernet2/0/7
!
interface FastEthernet2/0/8
!
interface FastEthernet2/0/9
!
interface FastEthernet2/0/10
!
interface FastEthernet2/0/11
!
interface FastEthernet2/0/12
!
interface FastEthernet2/0/13
!
interface FastEthernet2/0/14
!
interface FastEthernet2/0/15
!
interface FastEthernet2/0/16
!
interface FastEthernet2/0/17
!
interface FastEthernet2/0/18
!
interface FastEthernet2/0/19
!
interface FastEthernet2/0/20
!
interface FastEthernet2/0/21
!
interface FastEthernet2/0/22
!
interface FastEthernet2/0/23
!
interface FastEthernet2/0/24
!
interface FastEthernet2/0/25
!
interface FastEthernet2/0/26
!
interface FastEthernet2/0/27
!
interface FastEthernet2/0/28
!
interface FastEthernet2/0/29
```

```
!
interface FastEthernet2/0/30
!
interface FastEthernet2/0/31
!
interface FastEthernet2/0/32
!
interface FastEthernet2/0/33
!
interface FastEthernet2/0/34
!
interface FastEthernet2/0/35
!
interface FastEthernet2/0/36
!
interface FastEthernet2/0/37
!
interface FastEthernet2/0/38
!
interface FastEthernet2/0/39
!
interface FastEthernet2/0/40
!
interface FastEthernet2/0/41
!
interface FastEthernet2/0/42
!
interface FastEthernet2/0/43
!
interface FastEthernet2/0/44
!
interface FastEthernet2/0/45
!
interface FastEthernet2/0/46
!
interface FastEthernet2/0/47
!
interface FastEthernet2/0/48
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
!
interface GigabitEthernet2/0/4
!
interface Vlan1
 ip address 192.168.11.14 255.255.255.0
!
ip default-gateway 192.168.11.10
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip sla enable reaction-alerts
logging trap debugging
logging 192.168.42.124
```

```
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps energywise
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps rtr
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
```

```
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
!
monitor session 1 source interface Fa1/0/1
monitor session 1 destination interface Fa1/0/48
ntp clock-period 36029297
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

swan-3

```
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname SWAN-3
```

```
!
boot-start-marker
boot-end-marker
!
enable secret 5 <removed>!
username retail privilege 15 secret 5 <removed>
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PST recurring
switch 1 provision ws-c3750-48p
switch 2 provision ws-c3750-48p
system mtu routing 1500
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-1834566784
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1834566784
 revocation-check none
 rsakeypair TP-self-signed-1834566784
!
!
crypto pki certificate chain TP-self-signed-1834566784
 certificate self-signed 01
  <removed>   quit
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
```

```
!
ip ssh version 2
ip scp server enable
!
!
interface Loopback0
 no ip address
!
interface FastEthernet1/0/1
!
interface FastEthernet1/0/2
!
interface FastEthernet1/0/3
!
interface FastEthernet1/0/4
!
interface FastEthernet1/0/5
!
interface FastEthernet1/0/6
!
interface FastEthernet1/0/7
!
interface FastEthernet1/0/8
!
interface FastEthernet1/0/9
!
interface FastEthernet1/0/10
!
interface FastEthernet1/0/11
 description Link to ASA-WAN-1_1 SSM Port
!
interface FastEthernet1/0/12
!
interface FastEthernet1/0/13
!
interface FastEthernet1/0/14
!
interface FastEthernet1/0/15
!
interface FastEthernet1/0/16
!
interface FastEthernet1/0/17
!
interface FastEthernet1/0/18
!
interface FastEthernet1/0/19
!
interface FastEthernet1/0/20
!
interface FastEthernet1/0/21
!
interface FastEthernet1/0/22
!
interface FastEthernet1/0/23
!
interface FastEthernet1/0/24
!
interface FastEthernet1/0/25
!
interface FastEthernet1/0/26
!
interface FastEthernet1/0/27
!
interface FastEthernet1/0/28
```

```
!
interface FastEthernet1/0/29
!
interface FastEthernet1/0/30
!
interface FastEthernet1/0/31
!
interface FastEthernet1/0/32
!
interface FastEthernet1/0/33
!
interface FastEthernet1/0/34
!
interface FastEthernet1/0/35
!
interface FastEthernet1/0/36
!
interface FastEthernet1/0/37
!
interface FastEthernet1/0/38
!
interface FastEthernet1/0/39
!
interface FastEthernet1/0/40
!
interface FastEthernet1/0/41
!
interface FastEthernet1/0/42
!
interface FastEthernet1/0/43
!
interface FastEthernet1/0/44
!
interface FastEthernet1/0/45
!
interface FastEthernet1/0/46
!
interface FastEthernet1/0/47
!
interface FastEthernet1/0/48
!
interface GigabitEthernet1/0/1
 description link to RCORE-1 port G1/1
!
interface GigabitEthernet1/0/2
 description link to ASA-WAN-1_1 Port G0/1
!
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
!
interface FastEthernet2/0/1
!
interface FastEthernet2/0/2
!
interface FastEthernet2/0/3
!
interface FastEthernet2/0/4
!
interface FastEthernet2/0/5
!
interface FastEthernet2/0/6
!
interface FastEthernet2/0/7
```

```
!
interface FastEthernet2/0/8
!
interface FastEthernet2/0/9
!
interface FastEthernet2/0/10
!
interface FastEthernet2/0/11
 description Link to ASA-WAN-1_2 SSM Port
!
interface FastEthernet2/0/12
!
interface FastEthernet2/0/13
!
interface FastEthernet2/0/14
!
interface FastEthernet2/0/15
!
interface FastEthernet2/0/16
!
interface FastEthernet2/0/17
!
interface FastEthernet2/0/18
!
interface FastEthernet2/0/19
!
interface FastEthernet2/0/20
!
interface FastEthernet2/0/21
!
interface FastEthernet2/0/22
!
interface FastEthernet2/0/23
!
interface FastEthernet2/0/24
!
interface FastEthernet2/0/25
!
interface FastEthernet2/0/26
!
interface FastEthernet2/0/27
!
interface FastEthernet2/0/28
!
interface FastEthernet2/0/29
!
interface FastEthernet2/0/30
!
interface FastEthernet2/0/31
!
interface FastEthernet2/0/32
!
interface FastEthernet2/0/33
!
interface FastEthernet2/0/34
!
interface FastEthernet2/0/35
!
interface FastEthernet2/0/36
!
interface FastEthernet2/0/37
!
interface FastEthernet2/0/38
!
```

```
interface FastEthernet2/0/39
!
interface FastEthernet2/0/40
!
interface FastEthernet2/0/41
!
interface FastEthernet2/0/42
!
interface FastEthernet2/0/43
!
interface FastEthernet2/0/44
!
interface FastEthernet2/0/45
!
interface FastEthernet2/0/46
!
interface FastEthernet2/0/47
!
interface FastEthernet2/0/48
!
interface GigabitEthernet2/0/1
 description link to RCORE-2 port G1/1
!
interface GigabitEthernet2/0/2
 description link to ASA-WAN-1_2 Port G0/1
!
interface GigabitEthernet2/0/3
!
interface GigabitEthernet2/0/4
!
interface Vlan1
 ip address 192.168.11.13 255.255.255.0
!
interface Vlan40
 no ip address
!
ip default-gateway 192.168.11.10
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip sla enable reaction-alerts
logging trap debugging
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
```

```
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps energywise
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps rtr
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131 timeout 5
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
```

```
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication RETAIL
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport preferred none
 transport input ssh
 transport output none
!
end
```

VSG-Tenant-1-running

```
!Command: show running-config
!Time: Sat Apr 30 03:09:08 2011

version 4.2(1)VSG1(1)
no feature telnet
feature tacacs+

username admin password 5 <removed> role network-admin

banner motd #
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
#

ssh key rsa 2048
ip domain-lookup
ip domain-lookup
tacacs-server key 7 " <removed> "
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
hostname VSG-Tenant-1
no snmp-server protocol enable
snmp-server user admin network-admin auth md5 <removed> priv <removed> localizedkey
ntp source 192.168.41.63
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS

vrf context management
  ip domain-name cisco-irn.com
  ip name-server 192.168.42.130
  ip route 0.0.0.0/0 192.168.41.1
vlan 1
port-channel load-balance ethernet source-mac
port-profile default max-ports 32

vdc VSG-Tenant-1 id 1
  limit-resource vlan minimum 16 maximum 2049
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 32 maximum 32
  limit-resource u6route-mem minimum 16 maximum 16
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

interface mgmt0
  ip address 192.168.41.63/24

interface data0
  ip address 192.168.52.11/24
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
line vty
  exec-timeout 15
line console
  exec-timeout 15
boot kickstart bootflash:/nexus-1000v-kickstart-mz.VSG1.1.bin sup-1
boot system bootflash:/nexus-1000v-mz.VSG1.1.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-mz.VSG1.1.bin sup-2
boot system bootflash:/nexus-1000v-mz.VSG1.1.bin sup-2
ip access-list match-local-traffic
  ha-pair id 41

security-profile SecurityProfile-1@root/Tenant-1
  policy PolicySet-A@root/Tenant-1
  custom-attribute vnsporg "root/tenant-1"

security-profile default@root
  policy default@root
  custom-attribute vnsporg "root"
rule default/default-rule@root
  action 10 drop
rule PolicyA/allow_ICMP@root/Tenant-1
  condition 10 dst.net.ip-address eq 192.168.1.1
  condition 11 net.protocol eq 1
  action 10 log
  action 11 permit
policy default@root
  rule default/default-rule@root order 2
policy PolicySet-A@root/Tenant-1
  rule PolicyA/allow_ICMP@root/Tenant-1 order 101
```

```
vnm-policy-agent
  registration-ip 192.168.41.65
  shared-secret **********
  policy-agent-image bootflash:/vnmc-vsgpa.1.0.1j.bin
  log-level
logging logfile messages 2
logging server 192.168.42.124 6 facility local0
logging monitor 2
```