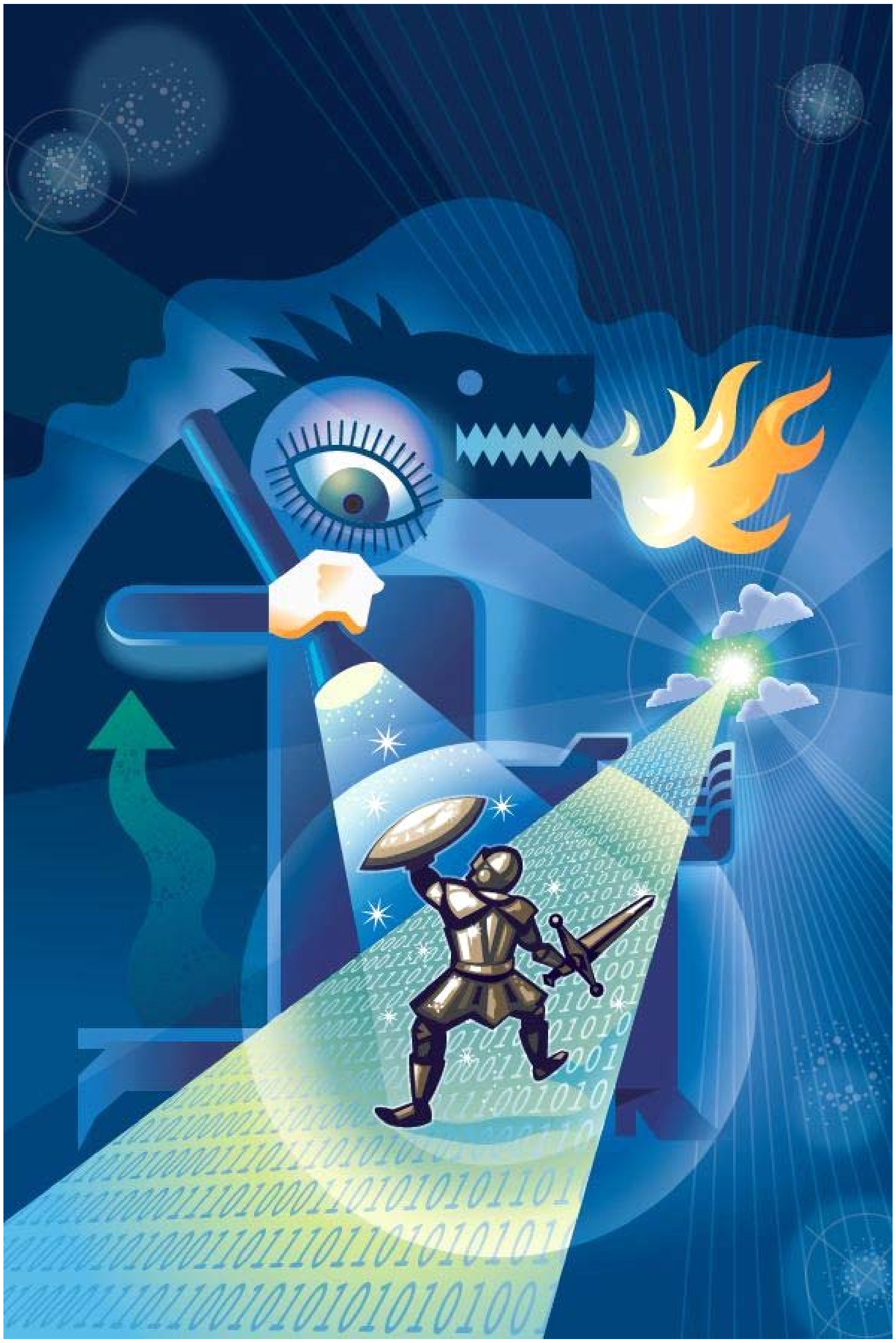
Cisco PCI Solution for Retail 2.0 Design Guide



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 3

CHAPTER 4

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

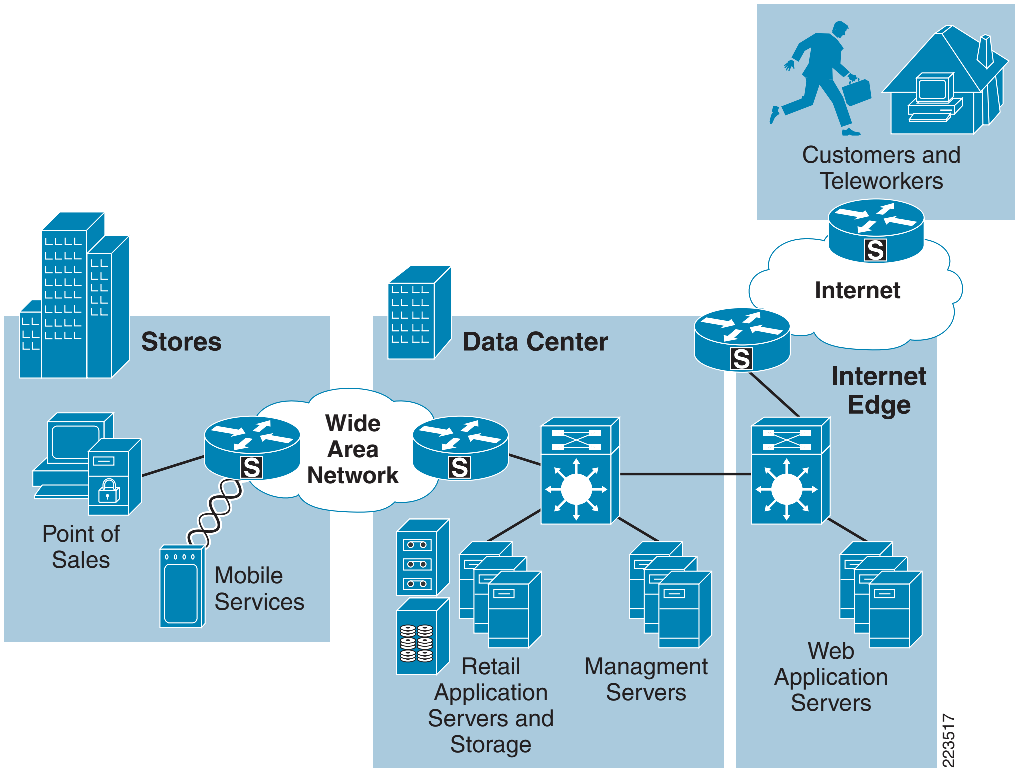
The Cisco PCI Solution for Retail 2.0 was developed to help retailers simplify and maintain PCI compliance. The solution consists of strategic guidance as well as tactical implementation. Cisco is in the unique position to apply its enterprise-wide architecture experience to the requirements of PCI. 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. Next, this document separates those architectures into their components. 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.

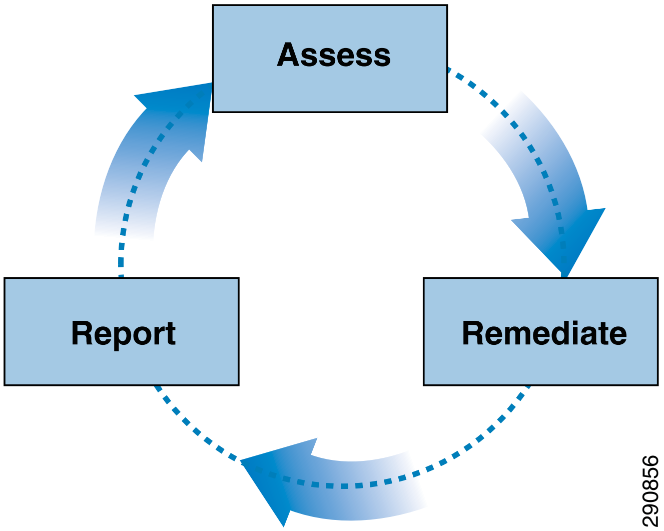
The Scoring Matrix has been replaced by a "Reporting Instructions" document. The necessary validation steps have been expanded. There is a greater level of detail required for assessor documentation (for example, observation of documentation, observation of process, action, or state, observation of configuration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

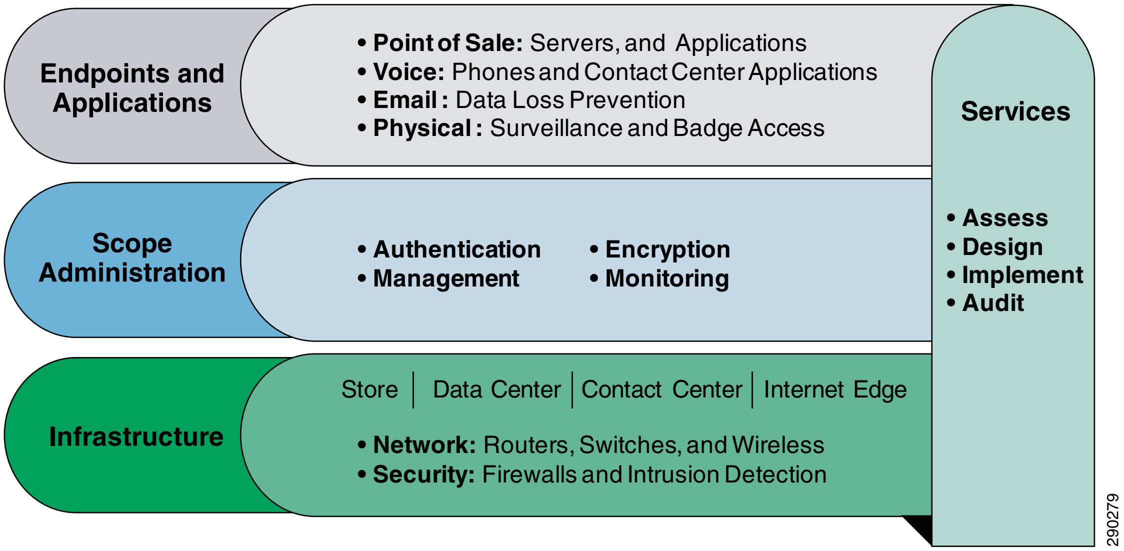
Internet

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

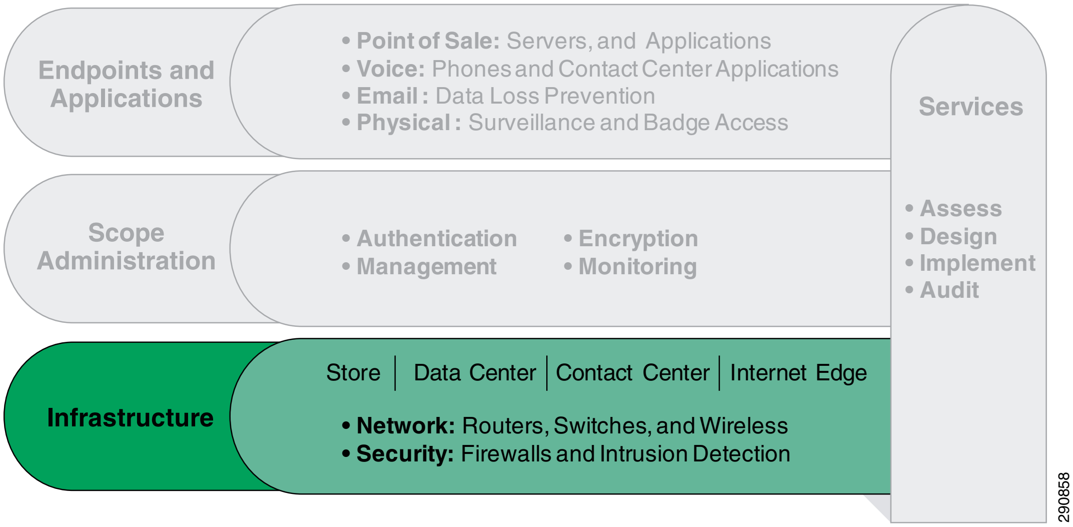
Solution Architecture

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 more information on the individual components used to build these architectures, see Chapter 4, "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

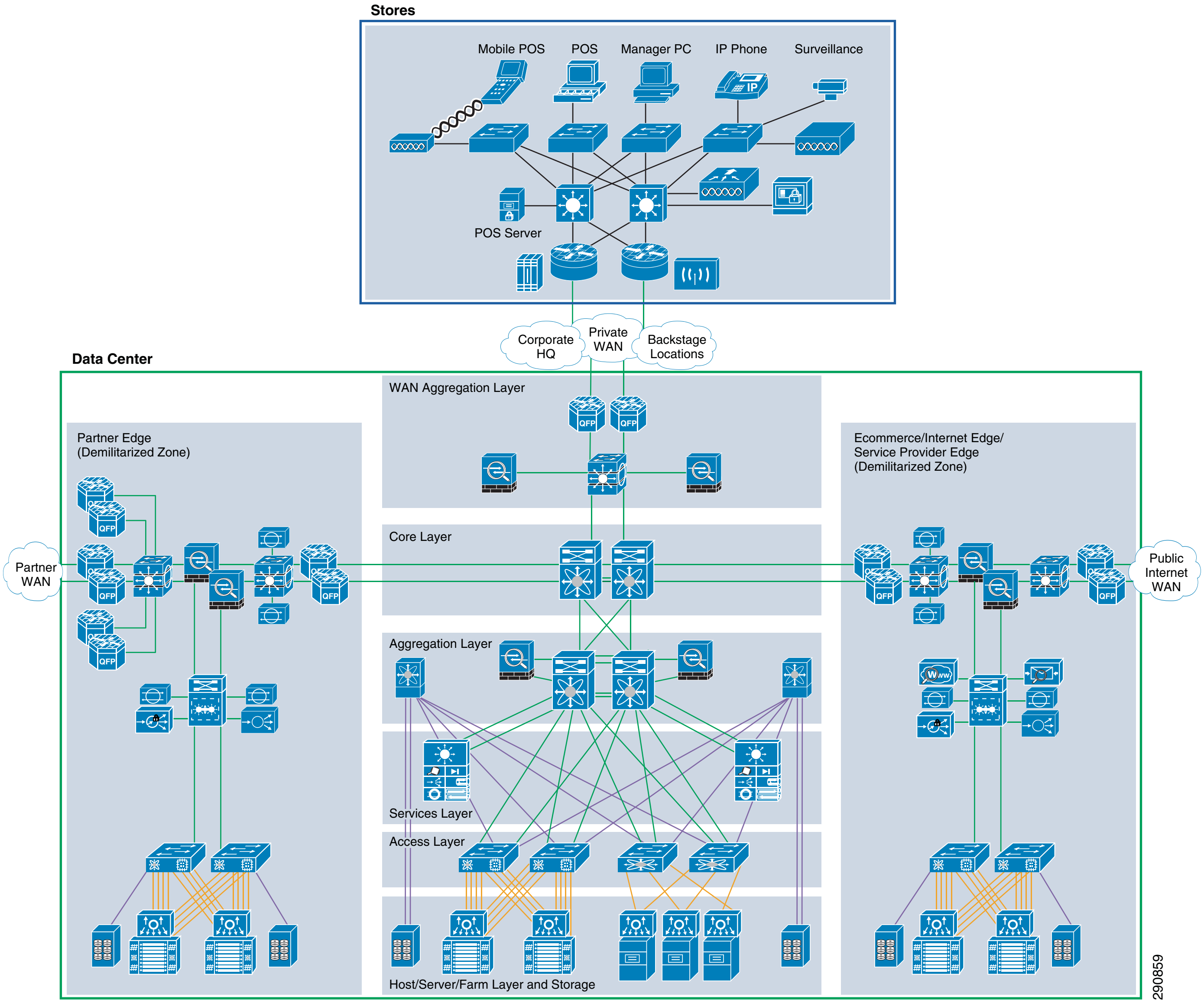

Endpoints and Applications
• Point of Sale: Servers, and Applications
• Voice: Phones and Contact Center Applications
• Email : Data Loss Prevention
• Physical : Surveillance and Badge Access
Services
Scope Administration
• Authentication
• Management
• Encryption
• Monitoring
• Assess
• Design
• Implement
• 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.

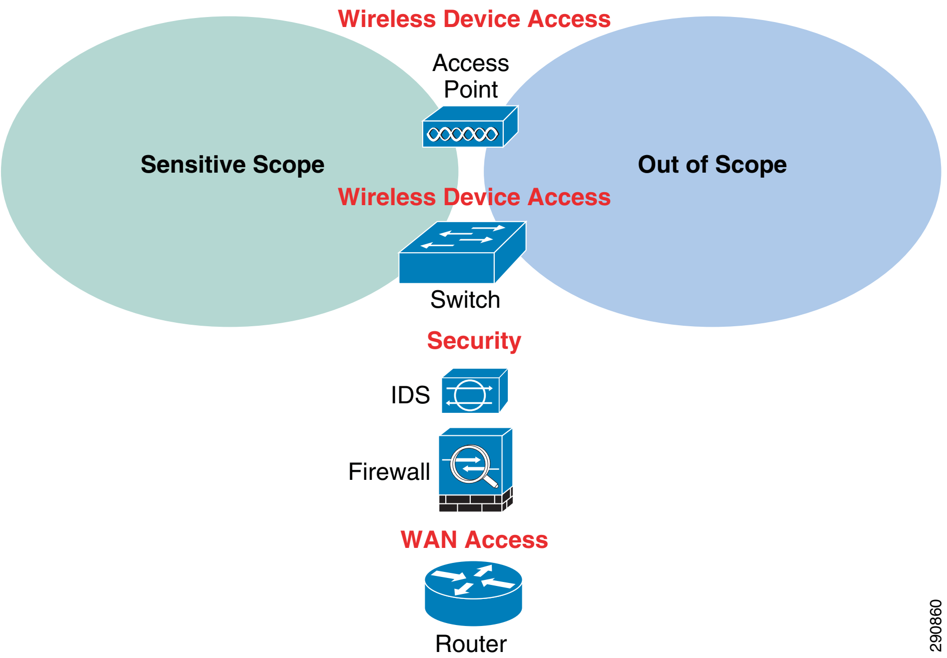
Store Architecture

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

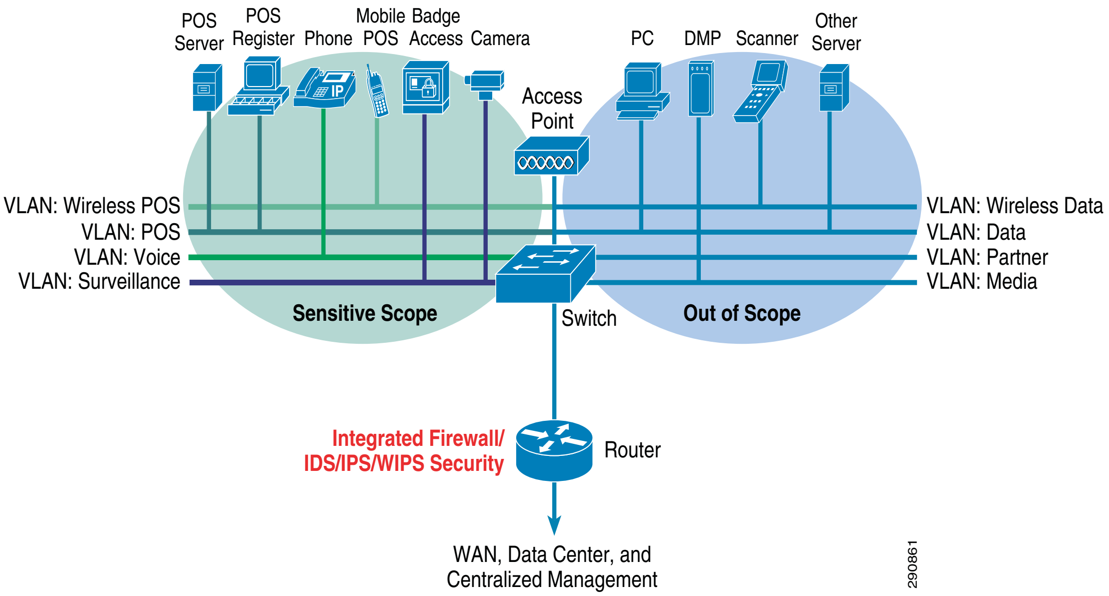
Table 3-1 Store Services and Corresponding Compliance Controls Located at Store (continued)

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.

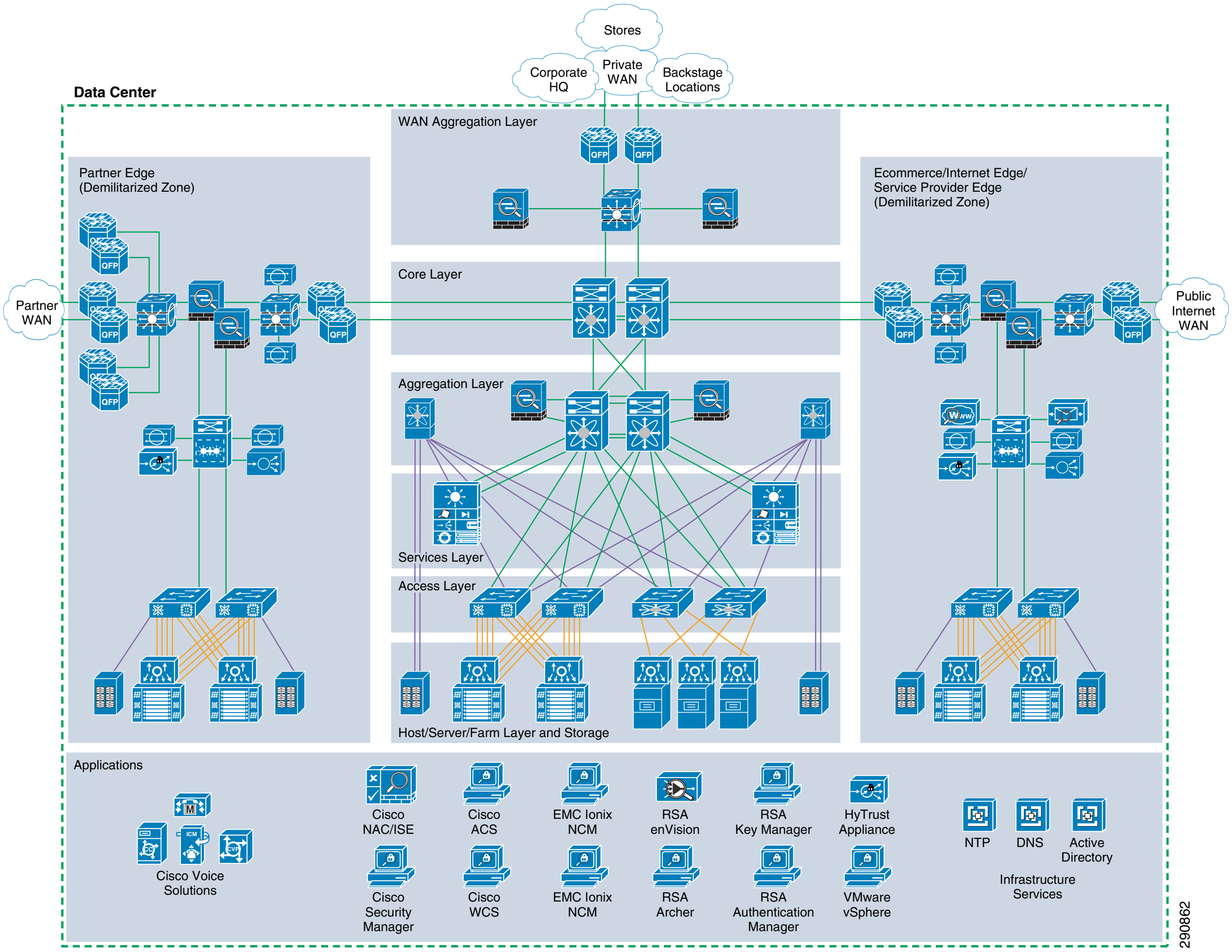
The remaining devices at the store level are considered *out-of-scope* and do not need to be audited, given that they are on their own network and segmented via firewall/IPS/IDS from the sensitive networks.

The PCI store model and its controls were applied to the small, medium, and large Connected Retail Store footprints. 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.

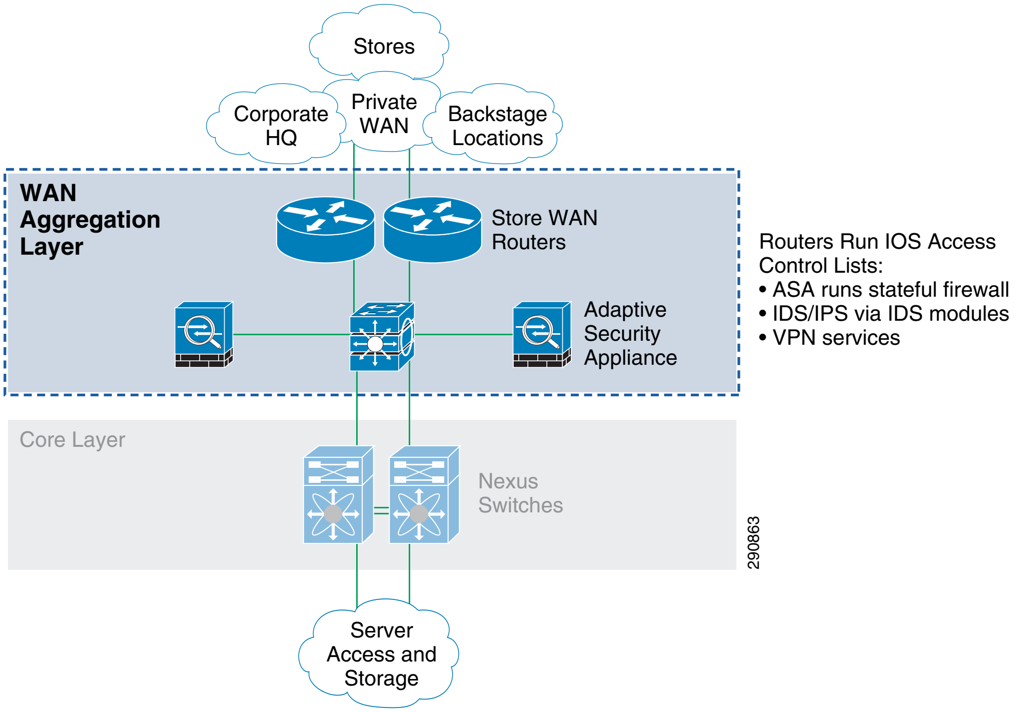
Data centers can house many types of functions, and the term itself can encompass narrow and broad aspects. For the purposes of this guide, data centers include the following functions:

- 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
Server Access and Storage
290863

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.

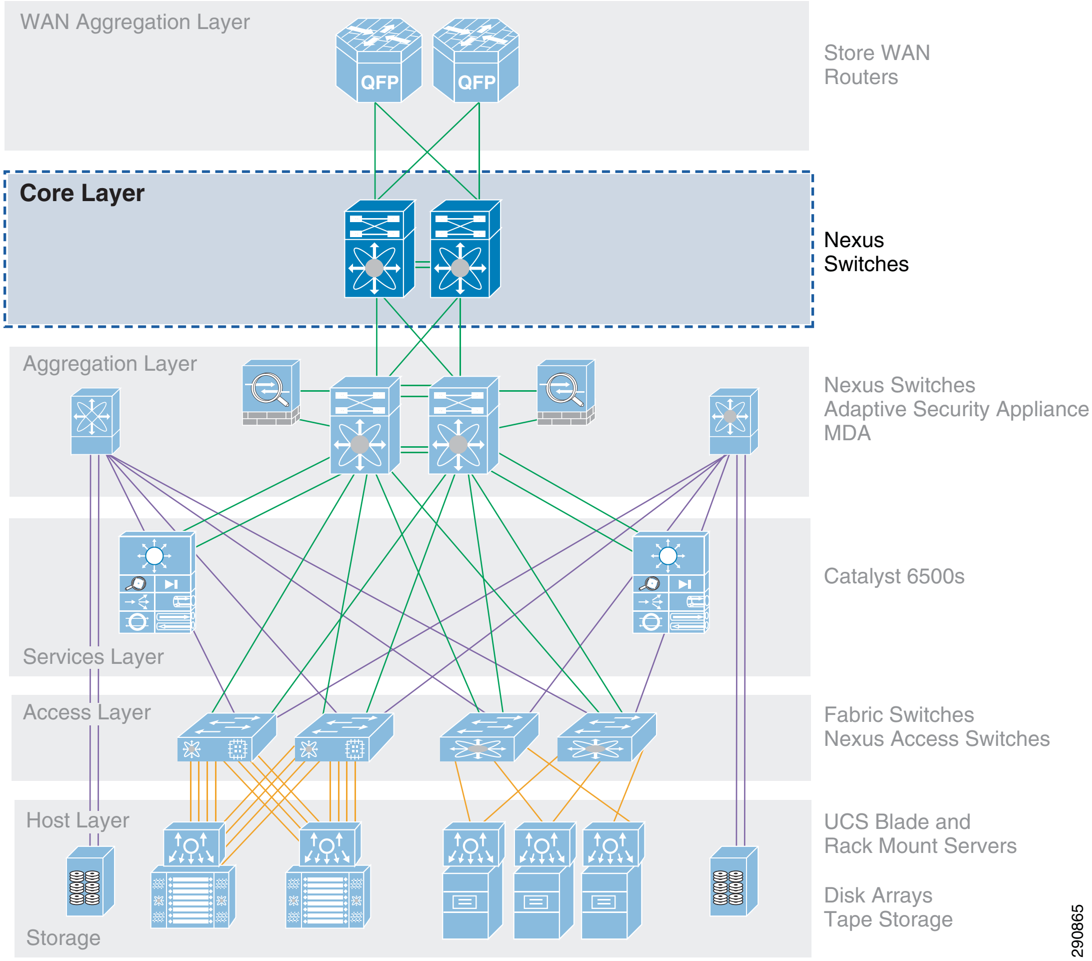
There are two typical WAN speeds categories for a WAN aggregation network: less than and up to OC3 (155 Mbps), and OC12 (622 Mbps) and above. The choice of these two network speeds determines the platform set to select from Cisco. In addition, this design creates two profiles for each WAN speed. These 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.

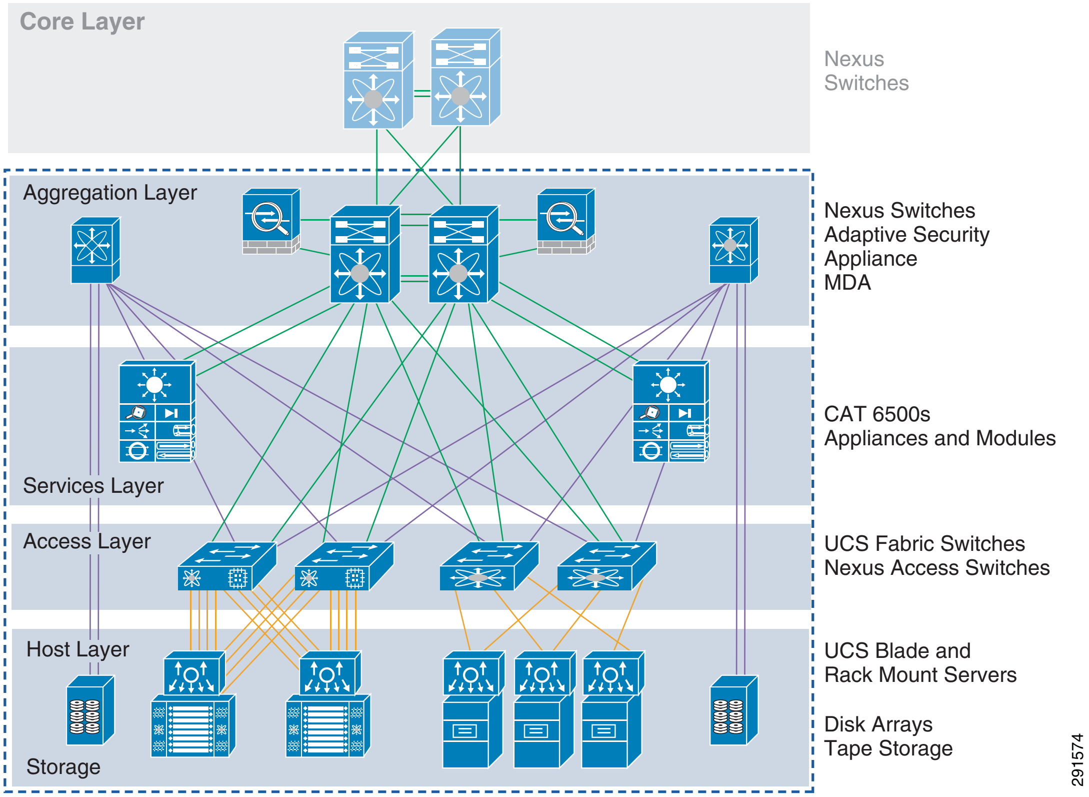
The core is not a perimeter; no security filtration should be performed at this layer.

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.

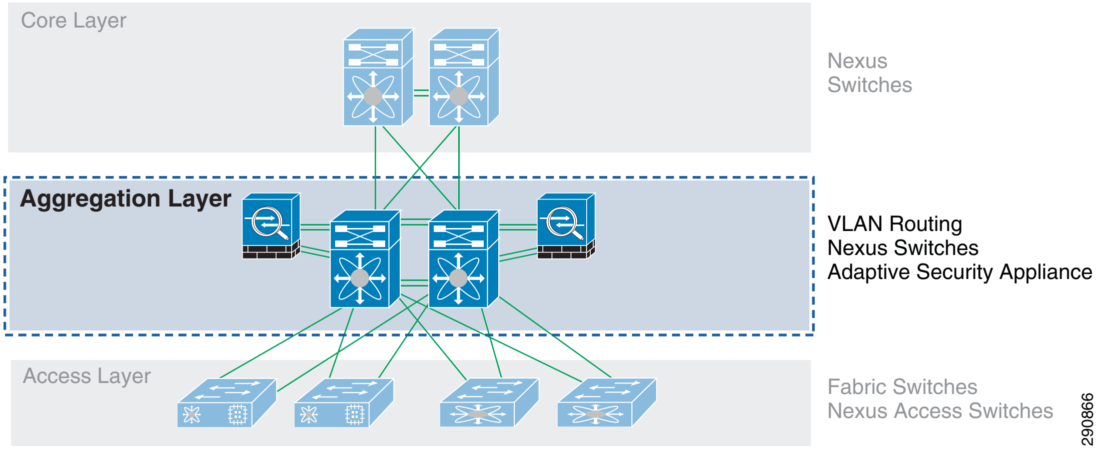
The layers that comprise the aggregation block are described in more detail below.

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



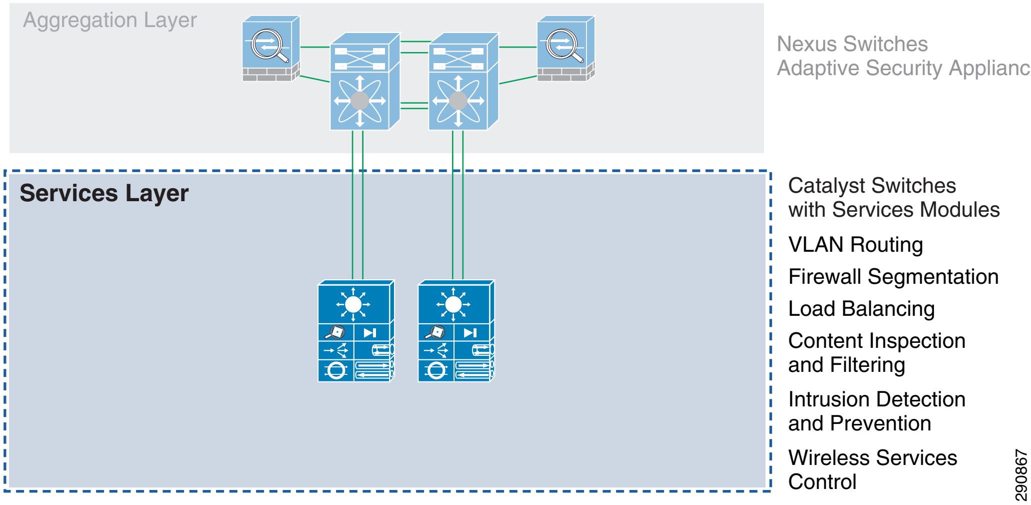
Design Considerations

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

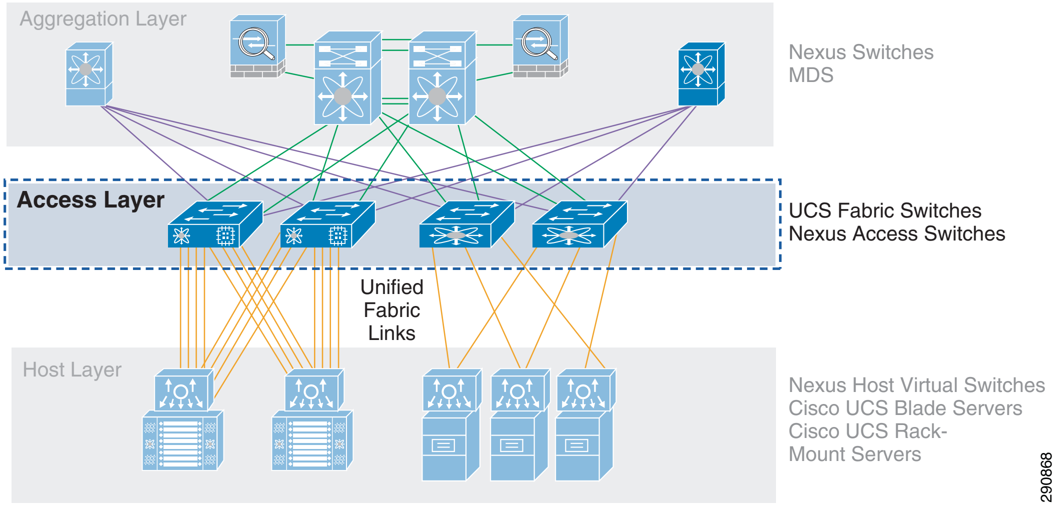
Services such as server load balancing and wide-area application services (WAAS) are used at this layer to optimize applications. Optimizing devices used within the scope of PCI are also brought into scope and are susceptible to the same controls as traditional network devices. For more information on understanding these controls, consult the capability assessment logic in Chapter 4, "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

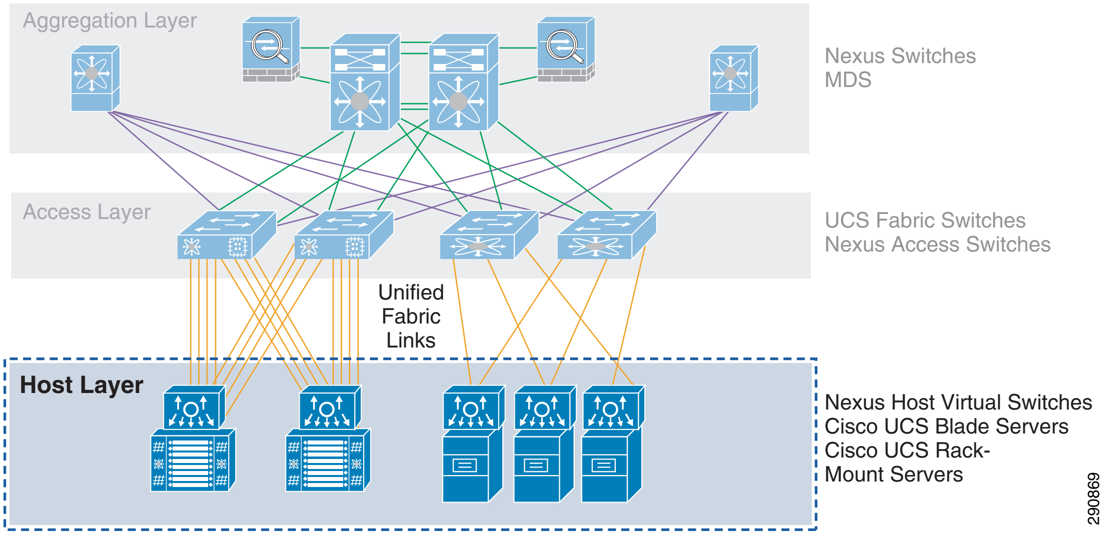
Switches provide both Layer 2 and Layer 3 topologies, fulfilling the various server broadcast domain or administrative requirements.

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.

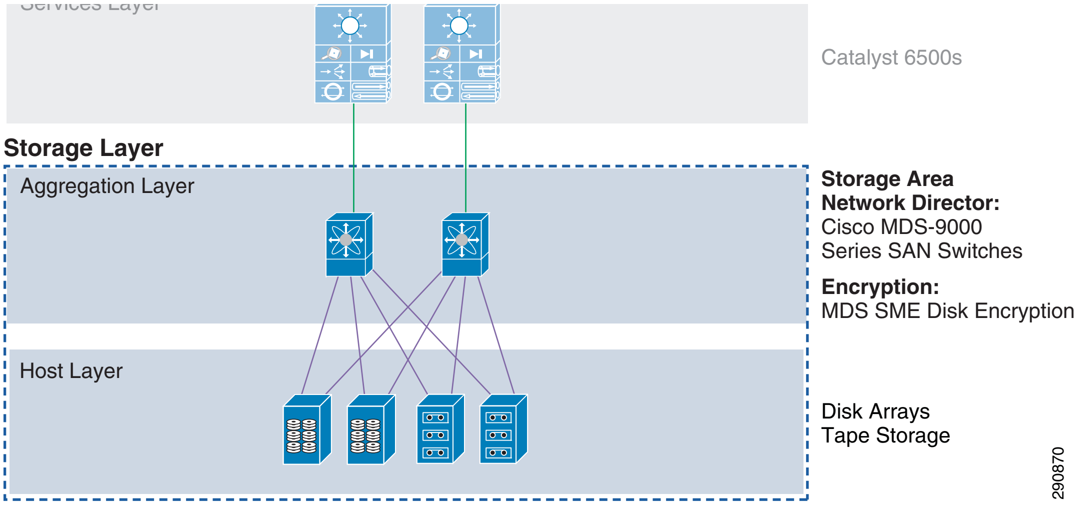
Table 3-2 Central Toolkit Description of Applications for Administrators

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.

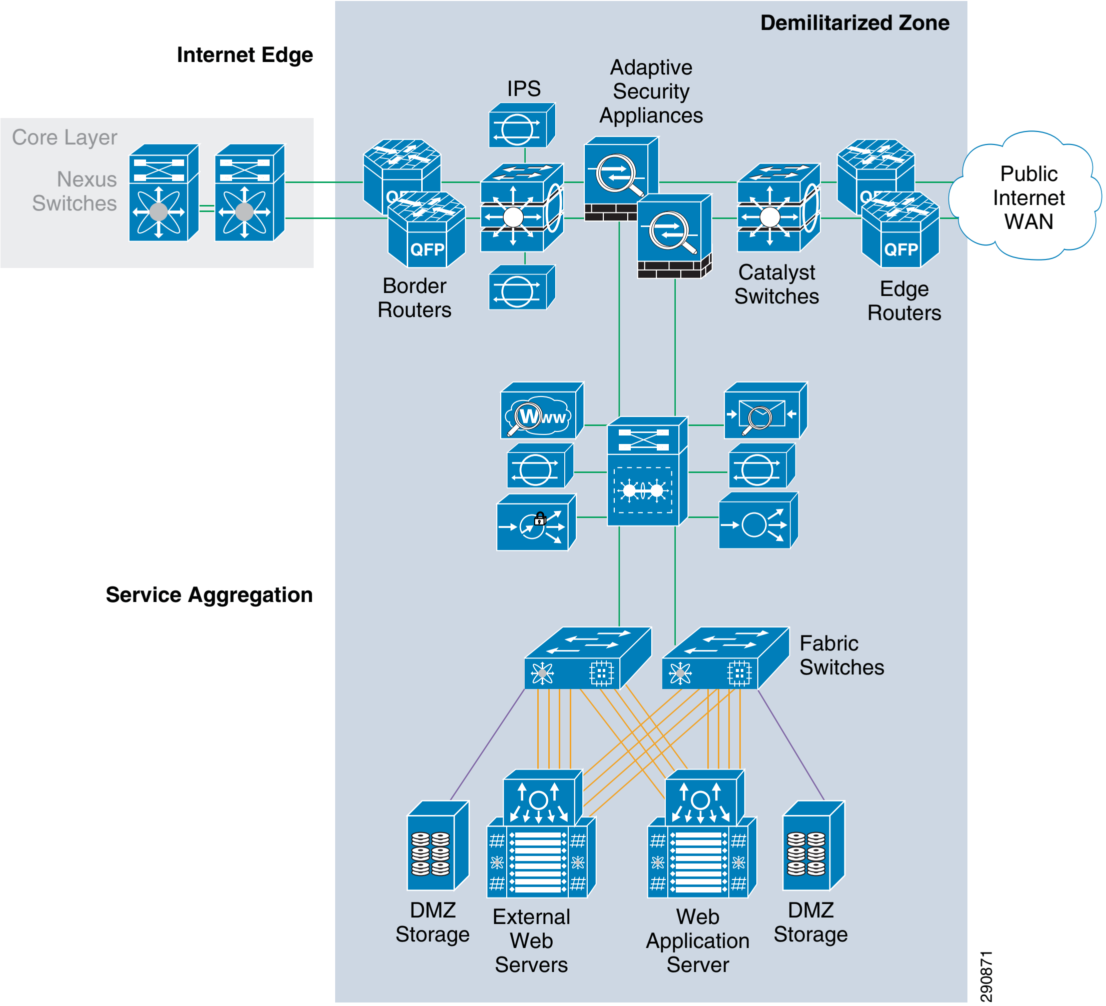
A subtle, yet potentially significant change to key management has been introduced with the PCI 2.0 standard. With past versions of the DSS, annual key rotations were required for encryption keys. DSS 2.0 now requires that keys are rotated at the end of their *cryptoperiod*, and references the NIST 800-57 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

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.

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 Summary

For each component, the PCI Assessment Summary table (see Table 4-1) lists each of the PCI sub-requirements that were passed, required compensating controls, or failed.

Table 4-1 PCI Assessment Summary Example

Models Assessed	
Cisco Catalyst Switch	
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

Table 4-1 PCI Assessment Summary Example

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 4-1.

Table 4-2 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 4-3 explains the color-codes icons used in the tables.

Table 4-3 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.

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

Table 4-5 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

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 4-6 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 4-6 lists the component assessment details for the Cisco Video Surveillance solution.

Table 4-7 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

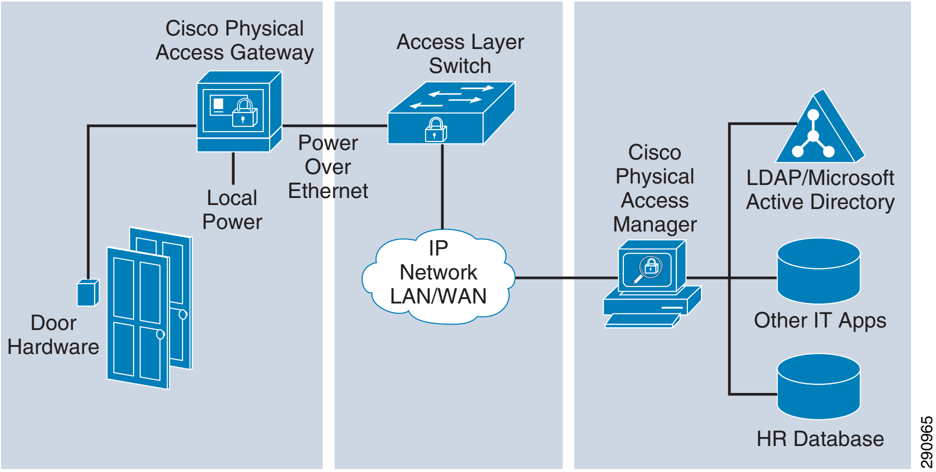
Cisco Physical Access Control

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 4-1). 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 4-1 ***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 4-8 ***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 4-8 lists the component assessment details for Cisco Physical Access Control.

Table 4-9 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

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

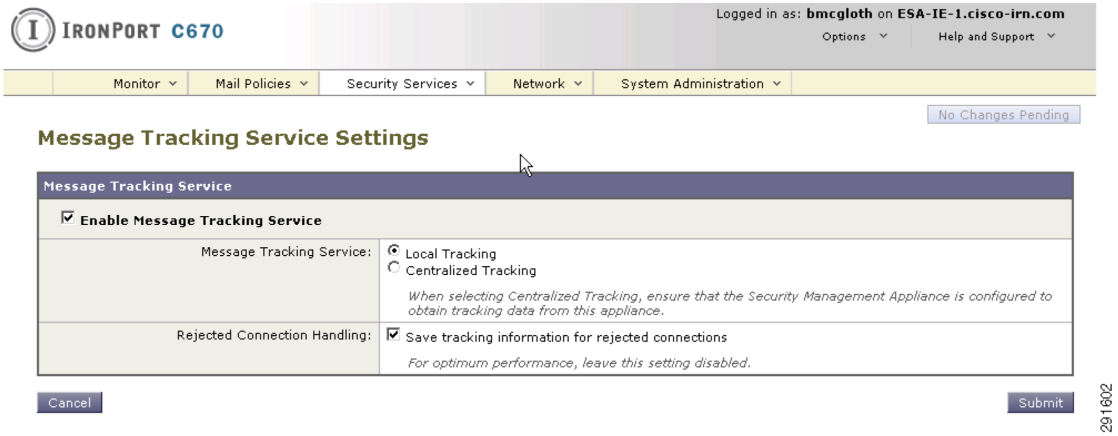
Primary PCI Function

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 4-2.

Figure 4-2 Enable IronPort Message Tracking



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

Message Tracking Service Settings

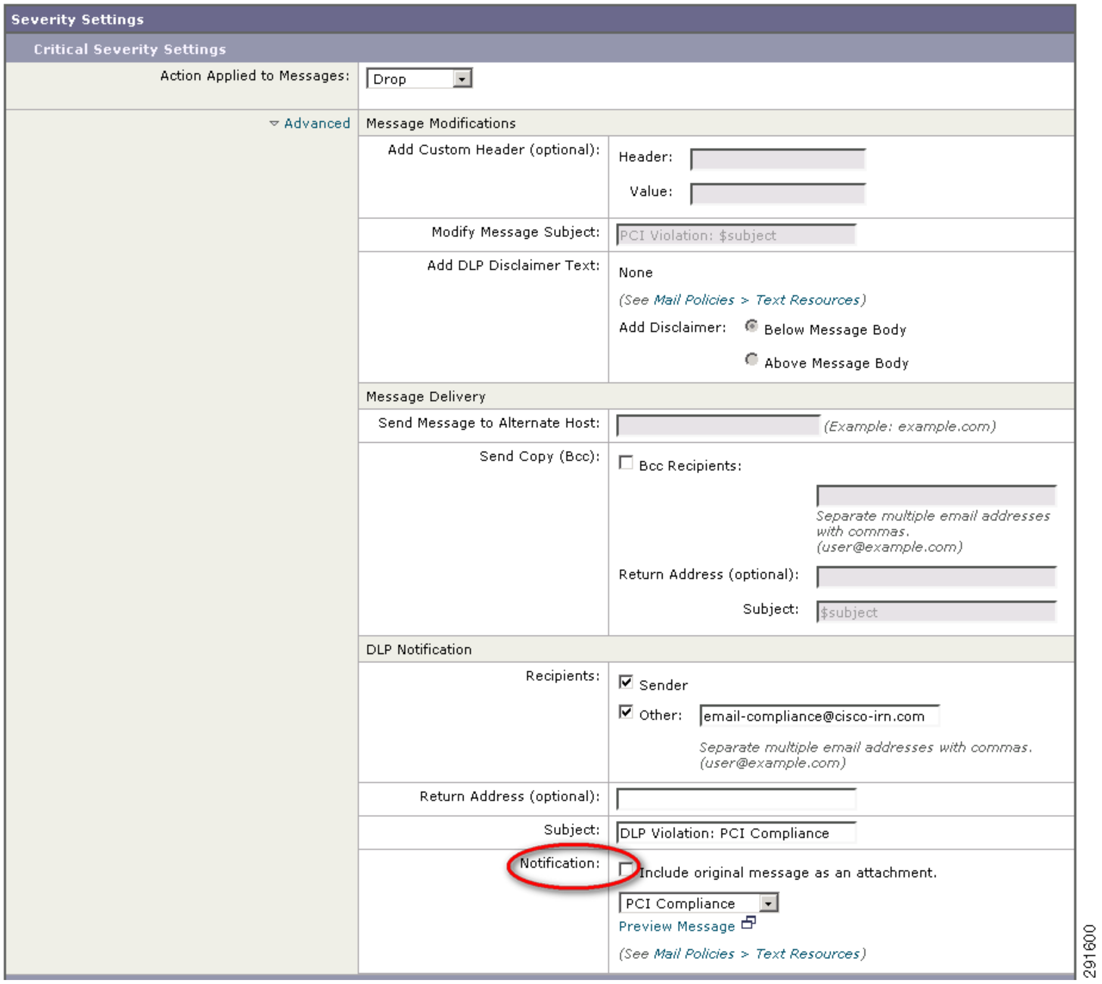
Message Tracking Service

☑ **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 4-3.

Figure 4-3 Policy in IronPort Excluding Original Message



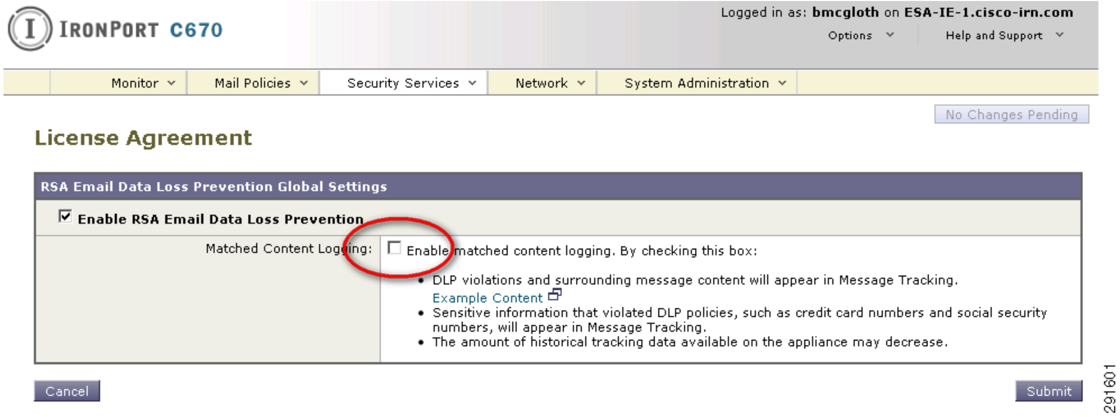
Severity Settings

Critical Severity Settings

Action Applied to Messages:	Drop	
	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 *(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 4-4. The local log of the IronPort server is not a safe encrypted place to store cardholder data.

Figure 4-4 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 4-10 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 4-10 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 4-10 lists the component assessment details for Cisco UCS.

Table 4-11 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

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 4-12 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 4-12 lists the component assessment details for the Cisco UCS Express and Cisco SRE.

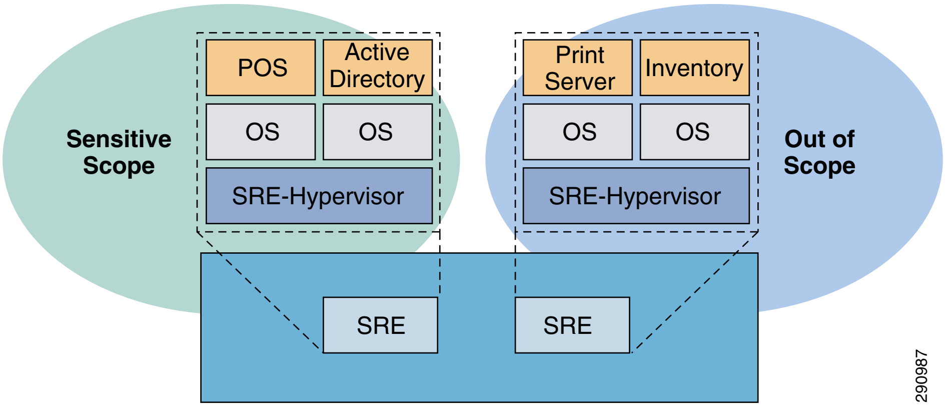
Table 4-13 Component Capability Assessment—Cisco UCS Express and Cisco SRE

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 4-5.)

Figure 4-5 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.

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 4-14 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 4-14 lists the component assessment details for Cisco Secure ACS.

Table 4-15 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

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 4-16 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 4-16 lists the component assessment details for RSA Authentication Manager.

Table 4-17 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/).

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 4-6 shows an example of a Cisco ISE-based TrustSec LAN deployment.

Figure 4-6 Cisco ISE-Based TrustSec LAN Deployment

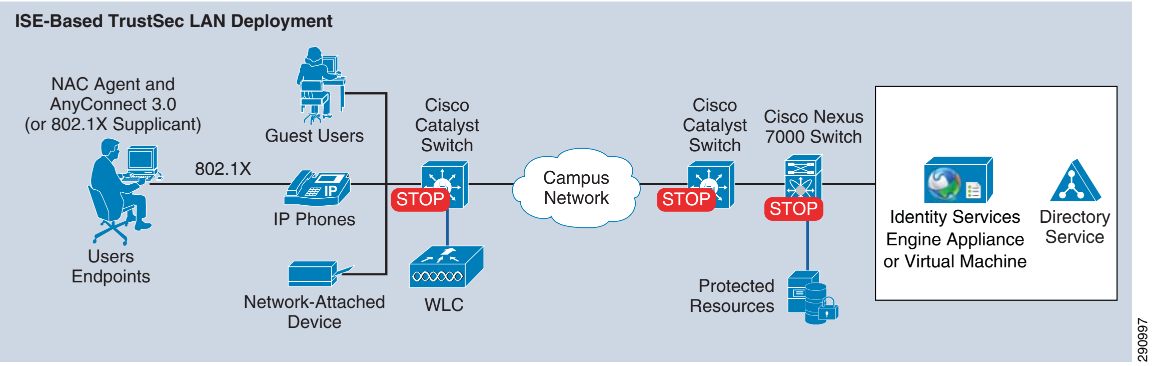


Table 4-18 PCI Assessment Summary—Cisco Identity Services Engine

Models Assessed
Cisco Identity Service Engine version 1.0.3.377
PCI Sub-Requirements Passed

Table 4-18 PCI Assessment Summary—Cisco Identity Services Engine

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
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 4-18 lists the component assessment details for the Cisco TrustSec Solution.

Table 4-19 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.

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 4-20 PCI Assessment Summary—Cisco Security Manager

Models Assessed	
Cisco Security Manager version 4.0.1	
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 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 4-20 lists the component assessment details for Cisco Security Manager.

Table 4-21 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.

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 4-22 PCI Assessment Summary—EMC Ionix NCM

Models Assessed
EMC Ionix Network Configuration Manager version 4.1.0.863 HF7

Table 4-22 PCI Assessment Summary—EMC Ionix NCM

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 4-22 lists the component assessment details for EMC Ionix Network Configuration Manager.

Table 4-23 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.

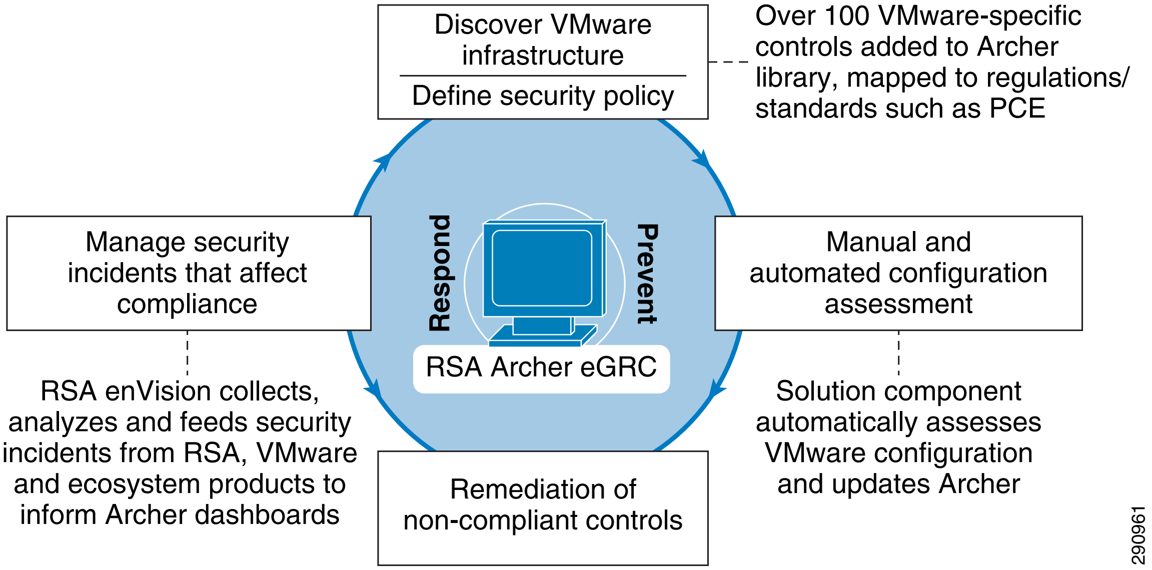
RSA Archer

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 4-7.)

Figure 4-7 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
Manual and automated configuration assessment
RSA Archer eGRC
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

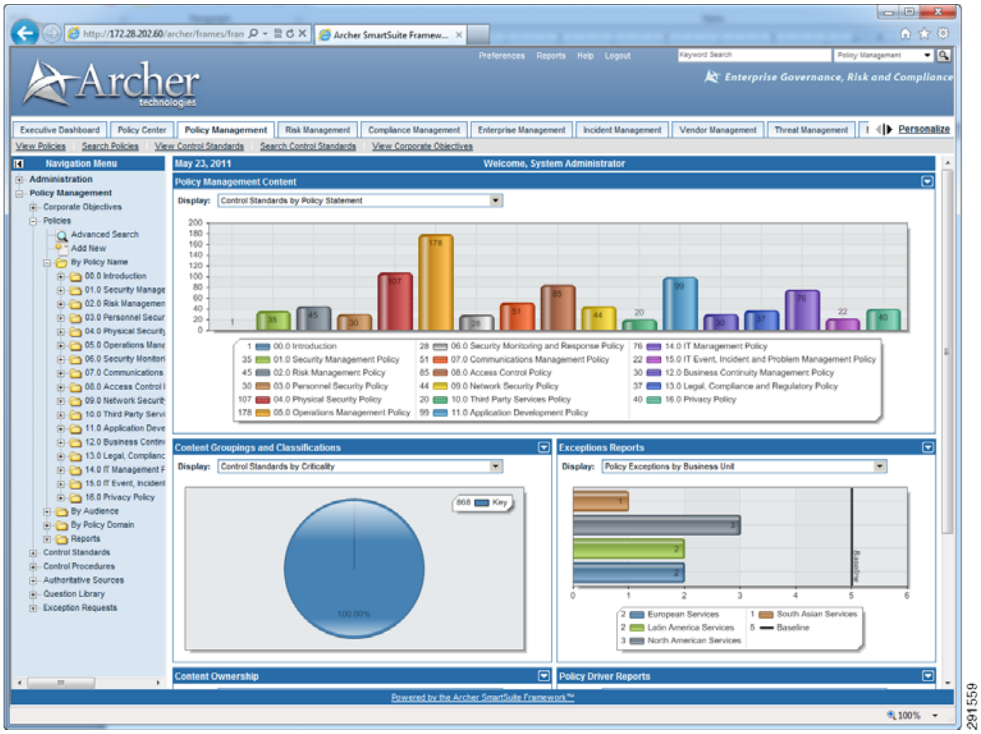
One of the major changes to PCI DSS 2.0 is its clarification on the use of virtualization technology in the cardholder data environment. If virtualization technology is used, the virtualization platform is always in scope for PCI. More than 130 control procedures in the Archer library have been written 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 4-8.

Figure 4-8 RSA Archer Policy Management


Archer technologies
Enterprise Governance, Risk and Compliance
Preferences Reports Help Logout
Executive Dashboard
Policy Center
Policy Management
Risk Management
Compliance Management
Enterprise Management
Incident Management
Vendor Management
Threat Management
Personalize
View Policies
Search Policies
View Control Standards
Search Control Standards
View Corporate Objectives
Navigation Menu
Administration
Policy Management
Corporate Objectives
Policies
Advanced Search
Add New
By Policy Name
By Audience
By Policy Domain
Reports
Control Standards
Control Procedures
Authoritative Sources
Question Library
Exception Requests
May 23, 2011
Welcome, System Administrator
Policy Management Content
Display: Control Standards by Policy Statement
1 00.0 Introduction
35 01.0 Security Management Policy
45 02.0 Risk Management Policy
30 03.0 Personnel Security Policy
107 04.0 Physical Security Policy
178 05.0 Operations Management Policy
28 06.0 Security Monitoring and Response Policy
51 07.0 Communications Management Policy
85 08.0 Access Control Policy
44 09.0 Network Security Policy
20 10.0 Third Party Services Policy
99 11.0 Application Development Policy
76 14.0 IT Management Policy
22 15.0 IT Event, Incident and Problem Management Policy
30 12.0 Business Continuity Management Policy
37 13.0 Legal, Compliance and Regulatory Policy
40 16.0 Privacy Policy
Content Groupings and Classifications
Display: Control Standards by Criticality
868 Key
100.00%
Exceptions Reports
Display: Policy Exceptions by Business Unit
Baseline
2 European Services
2 Latin America Services
3 North American Services
1 South Asian Services
5 Baseline
Content Ownership
Policy Driver Reports
Powered by the Archer SmartSuite Framework™
100%
291559

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 4-24 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 4-24 lists the component assessment details for RSA Data Protection Manager.

Table 4-25 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

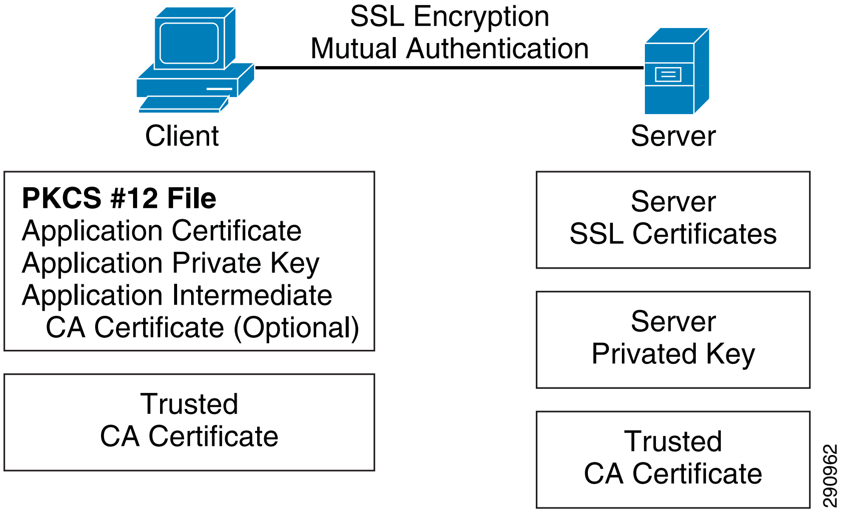
RSA Data Protection Manager's encryption and key management capabilities can be used to store the data in a compliant manner. RSA Data Protection Manager provides application development libraries that support a wide range of development languages and enables developers to easily integrate encryption 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 4-9.)

Figure 4-9 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.

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 4-26 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
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 4-26 lists the component assessment details for the EMC SAN disk array.

Table 4-27 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.

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 4-28 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 4-28 lists the component assessment details for RSA enVision.

Table 4-29 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.

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 4-30 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 4-30 lists the component assessment details for the HyTrust Appliance.

Table 4-31 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).

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 4-1.

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 4-32 lists the performance of the Cisco ISR in satisfying PCI sub-requirements.

Table 4-32 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.	

Table 4-32 PCI Assessment Summary—Cisco ISR

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.

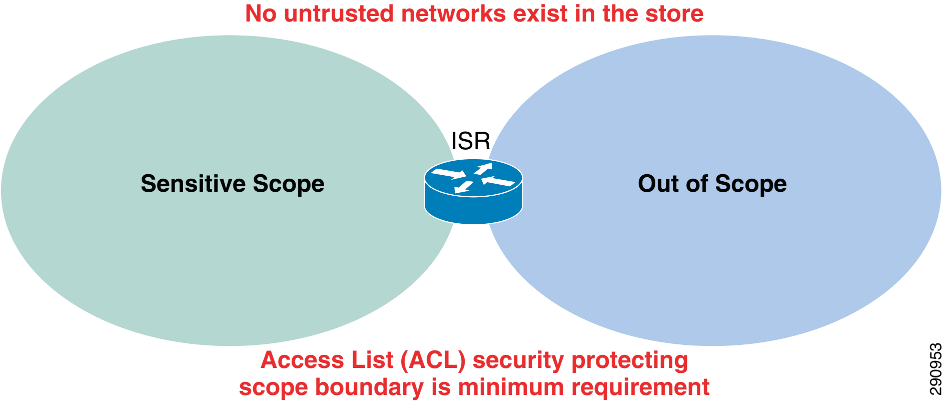
1. As a router, directing traffic between networks

   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 4-10.)

Figure 4-10 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:

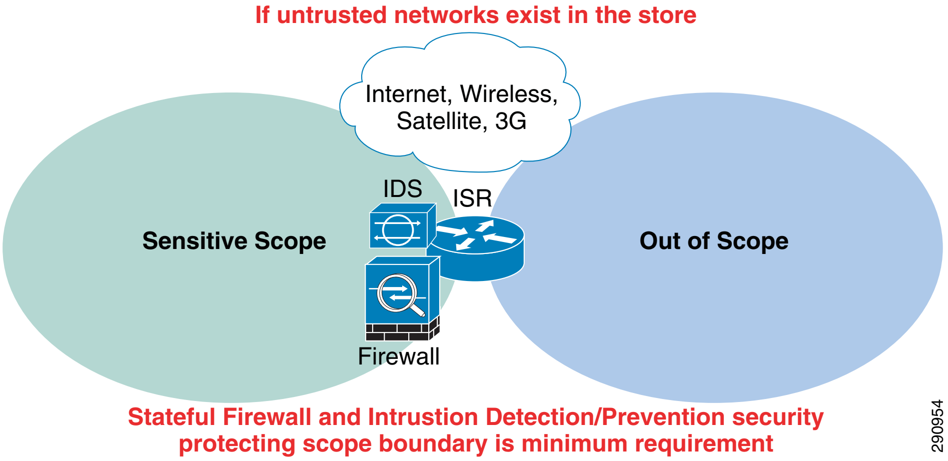
   - The Internet
   - Wireless

- 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 4-11.)

Figure 4-11 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 4-32 lists the component assessment details for the Cisco ISR.

Table 4-33 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 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

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 4-34 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 4-34 lists the component assessment details for the Cisco data center routers.

Table 4-35 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

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 4-36 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
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

Table 4-36 PCI Assessment Summary—Store Switches

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.	

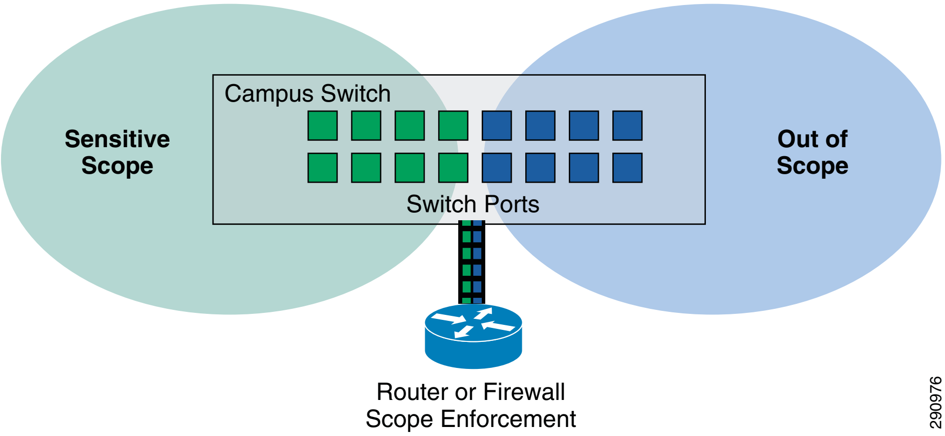
Primary PCI Function

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 4-12 shows an example of switch segmentation.

Figure 4-12 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 4-36 lists the component assessment details for the Cisco store switches.

Table 4-37 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.

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.

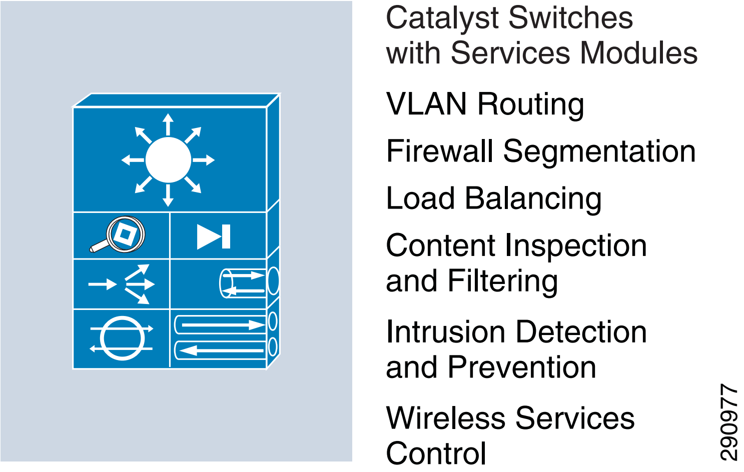
Table 4-38 PCI Assessment Summary—Cisco Catalyst Data Center Switches

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 4-13.)

Figure 4-13 Cisco Catalyst Data Center Switches


Catalyst Switches with Services Modules
VLAN Routing
Firewall Segmentation
Load Balancing
Content Inspection and Filtering
Intrusion Detection and Prevention
Wireless Services Control
290977

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 4-38 lists the component assessment details for the Cisco Catalyst data center switches.

Table 4-39 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.

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 4-40 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.	
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 4-40 lists the component assessment details for the Cisco Nexus 1000V Series Switch.

Table 4-41 Component Capability Assessment—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.

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 4-42 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
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 4-42 lists the component assessment details for the Cisco Nexus data center switches.

Table 4-43 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.

Cisco 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 4-44 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
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 4-44 lists the component assessment details for Cisco wireless products.

Table 4-45 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 4-46.

Table 4-46 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

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 4-47 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 4-47 lists the component assessment details for Cisco MDS storage switches.

Table 4-48 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

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 4-49 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 4-49 lists the component assessment details for the Cisco ASA 5500 Series.

Table 4-50 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.

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 4-51 PCI Assessment Summary—Cisco ASA 5500 Series (Data Center)

Models Assessed	
ASA5540 w/SSM-40 ASA5540 w/SSM-20 ASA5585-S60-2A-K9	asa841-k8.bin asa841-k8.bin 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	
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 4-51 lists the component assessment details for Cisco ASA 5500 Series.

Table 4-52 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.

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 4-53 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 4-53 lists the component assessment details for the Cisco FWSM.

Table 4-54 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.

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 4-55 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 4-55 lists the component assessment details for the Cisco VSG.

Table 4-56 Component Capability Assessment—Cisco VSG

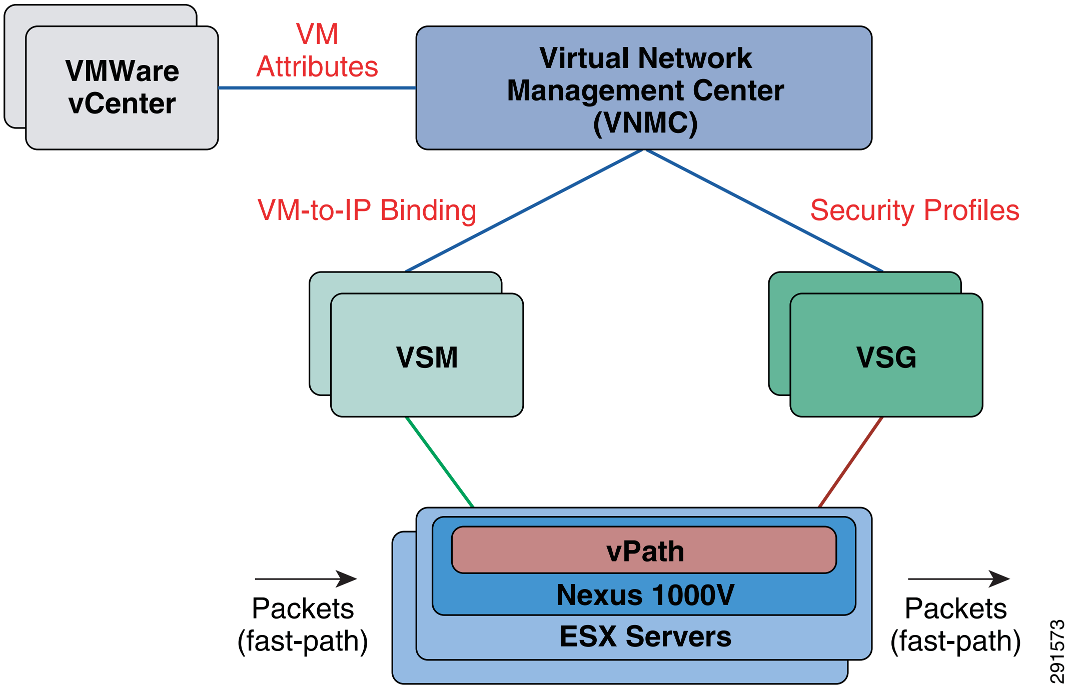
Cisco VSG	
PRIMARY FUNCTION	Requirement 1 (1.2, 1.3)
Restrict traffic between the cardholder data environment and other network areas.	
CAPABILITY	ASSESSMENT
Secure Services	
Disabled any unnecessary services—*“Enable only necessary and secure services, protocols, daemons, etc., as required for the function 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 4-14 Cisco Nexus VSG System Architecture



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 4-57 PCI Assessment Summary—Cisco IDSM2

Models Assessed
WS-SVC-IDSM-2 version 7.0(4)

Table 4-57 PCI Assessment Summary—Cisco IDSM2

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 4-57 lists the component assessment details for the Cisco ISDM2.

Table 4-58 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

CHAPTER 5

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 5-1 provides a summary of the PCI assessment results.

Table 5-1 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		

PCI
PCI
ADVANCED HACKING
CREDIT CARD NO'S
LARRY JANOFF ©
"THEY don't sleep at night"
Larry Janoff