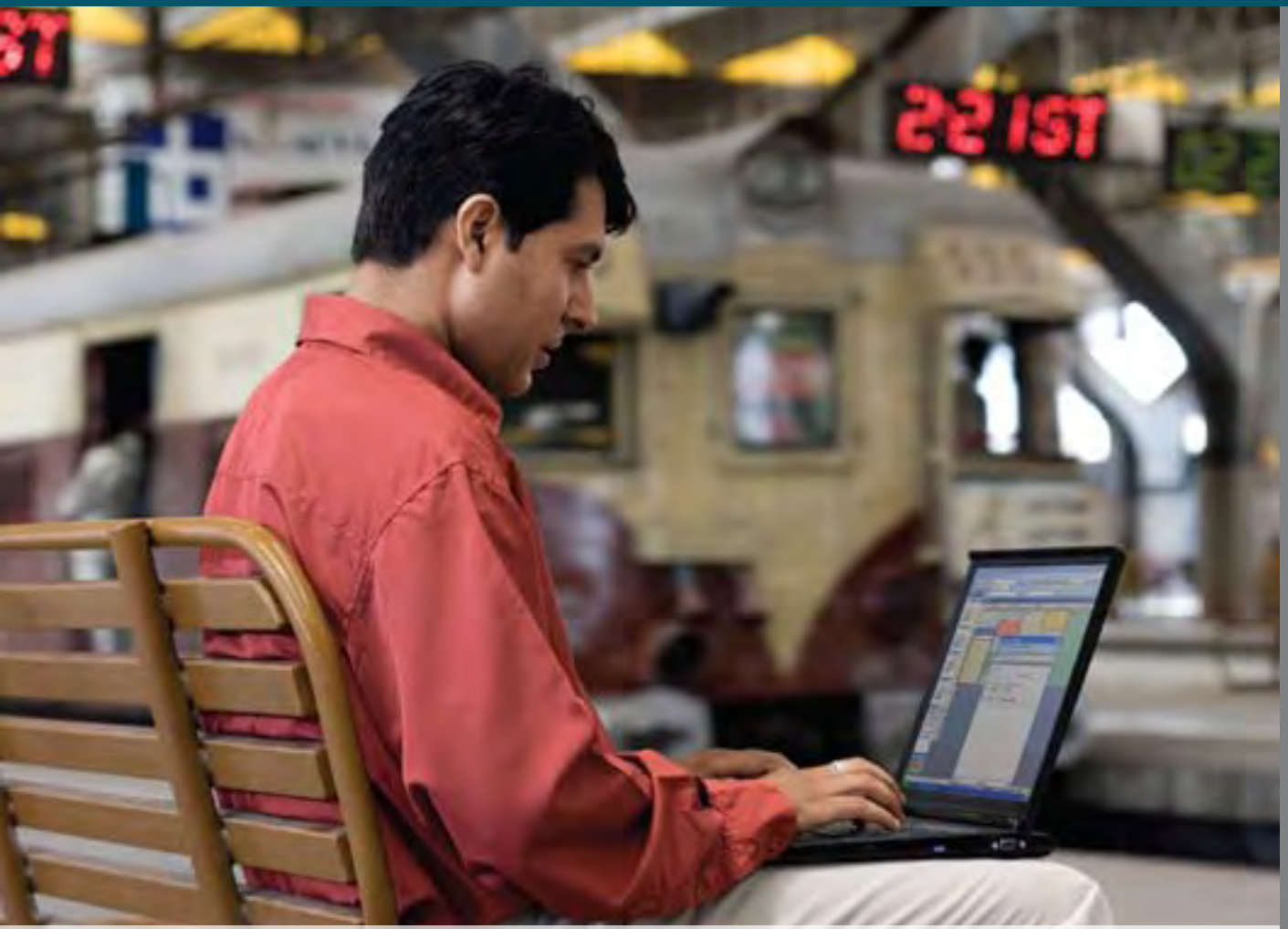
Quick Reference Guide
For Customers

Cisco® Security Solutions



January 2009

Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Why Security Matters More Than Ever

HOME

Maintain Reputation

Today's security challenges put organizations at risk. One data breach can ruin your positive reputation with customers, investors, and the marketplace.

Meet Regulatory Compliance Requirements

Every company is subject to some sort of regulation, often related to privacy and protection of customer information. Compliance dictates strong and thoughtful security.

Protect Business Information

Information is at the core of every organization. The availability, integrity, and confidentiality of critical assets must be protected wherever they reside.

Optimize Business Operations

Most companies have difficulty determining the cost of a day of downtime because of the number of direct and indirect factors that must be considered. Among these are lost productivity, loss of business and loyalty, impact on reputation and brand, cost of repair and recovery, and potential legal liability.

The Cisco® Self-Defending Network

For organizations that need to reduce their security and compliance IT risk while decreasing IT administrative burden and reducing total cost of ownership, Cisco provides leading security in a systems approach. Unlike other security vendors, only Cisco offers the benefits of a best-of-breed approach combined with a systems approach:

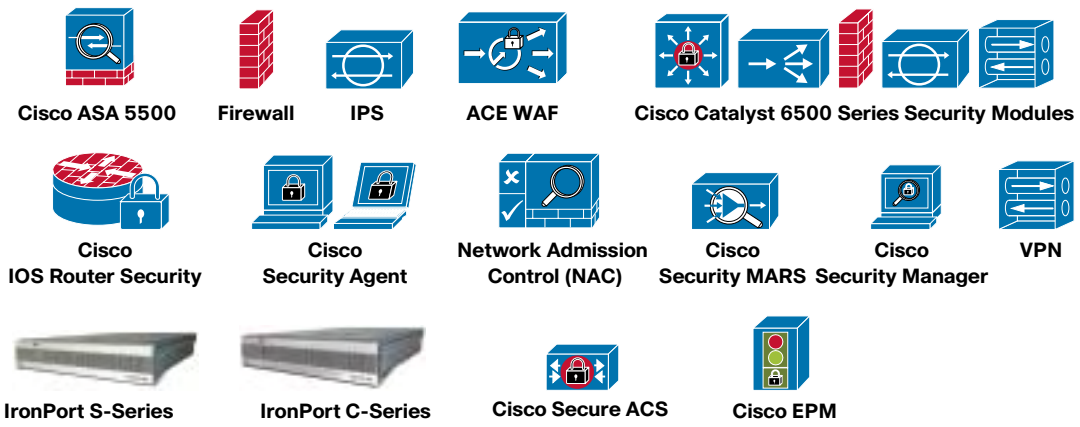
- Best-of-breed security addresses emerging threats
- Systems approach addresses pervasive threats, aids in meeting compliance regulations, and enables cost-effective management
- History of security innovations since 1995
- Network security market leadership position in firewall technology, virtual private networking, email and web security, and intrusion prevention
- Award-winning products
- Customer validation and success

Why Cisco?

Cisco offers the broadest and deepest product and services portfolios, and our partners are empowered to design and implement a solution customized to your unique requirements.

For more information, please visit:
http://www.cisco.com/go/securitysolutions

The following figure provides a quick look at Cisco security solutions.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Cisco ASA 5500 Series Adaptive Security Appliances

Overview

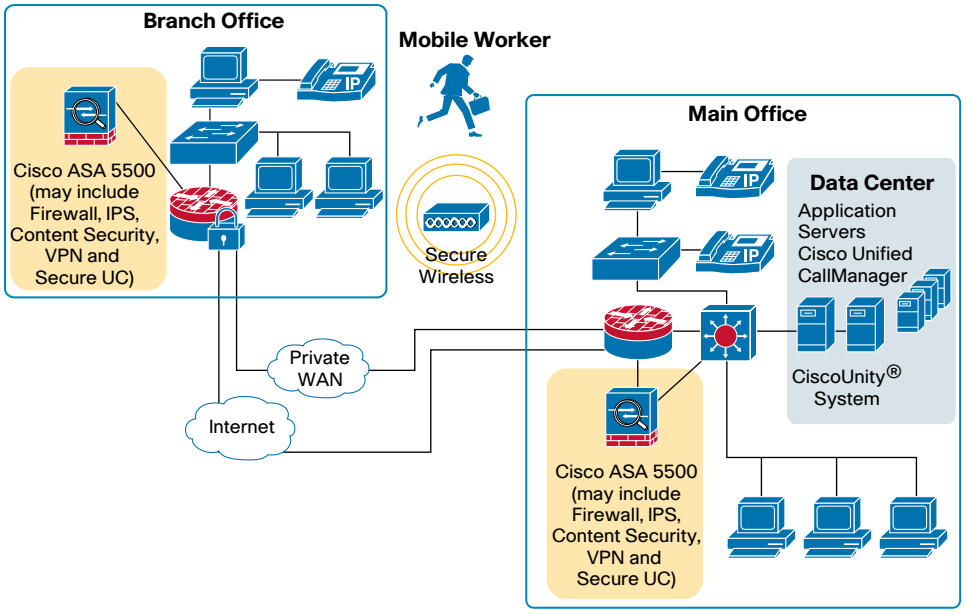
- The Cisco® ASA 5500 Series converges full-featured, high-performance firewall (including application firewall services), intrusion prevention, content security, IPsec/ SSL VPN, and secure unified communications technologies in a single, easy-to-use security appliance.
- Now you can provide industrial-strength security for your network while reducing cost and complexity by converging multiple security functions into a high-performance appliance.
- Cisco ASA 5500 Series integrated security platforms provide the scalability to meet the security needs of businesses of all sizes.

Benefits

- Reduces cost and complexity by providing firewall, SSL and IPsec VPN, intrusion prevention, network content security services, and secure unified communications on a single hardware platform
- Delivers high performance with multiple security services for the same cost as a firewall alone
- Adapts to new security threats
- Provides thorough remote-office protection to protect data and voice for remote workers
- Provides an integrated threat protection solution on a single device, for both SSL and IPsec VPN connectivity

For more information, please visit:
http://www.cisco.com/go/asa

The following figure shows how Cisco ASA 5500 Series Adaptive Security Appliances fit in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Firewall

HOME

Overview

The firewall protects the resources of a private network from unauthorized access to applications, networks, and data by internal or external users.

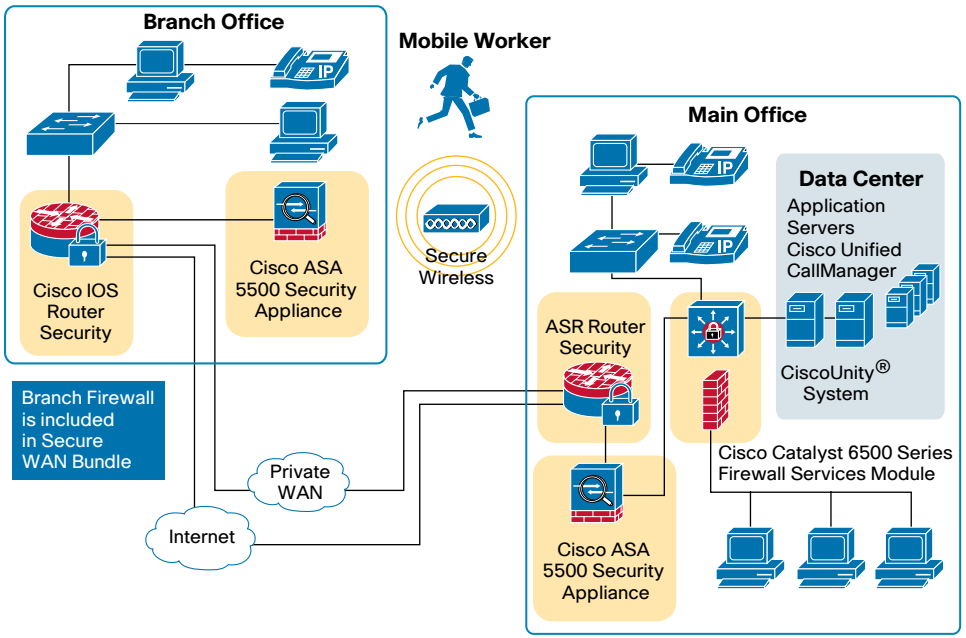
- Cisco® firewall solutions provide integrated network security services, including:
  - Stateful packet inspection
  - Application-layer and protocol inspection
  - Inline intrusion prevention
  - Rich multimedia and voice security
- Cisco offers multiple firewall solutions, including:
  - Cisco ASA 5500 Series Adaptive Security Appliances
  - Cisco IOS® Software- and Cisco NX-OS® Software-based firewall on Cisco routers
  - Cisco Catalyst® 6500 Series Firewall Services Module (FWSM) for environments needing greater scalability

Benefits

- Enables organizations of all sizes to protect their critical networks from unauthorized access
- Protects applications and network services from attack with advanced application inspection capabilities
- Offers multiprotocol support to enable dynamic routing for improved network reliability and performance
- Makes it easy to centrally administer and manage all firewall solutions using Cisco Security Manager
- Provides an extremely resilient security infrastructure with high-availability capabilities
- Maximizes network uptime, resulting in improved productivity
- Enables secure deployment of next-generation unified communications and multimedia applications

For more information, please visit:
http://www.cisco.com/go/firewall

The following figure shows how Cisco firewall solutions fit in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Intrusion Prevention Systems

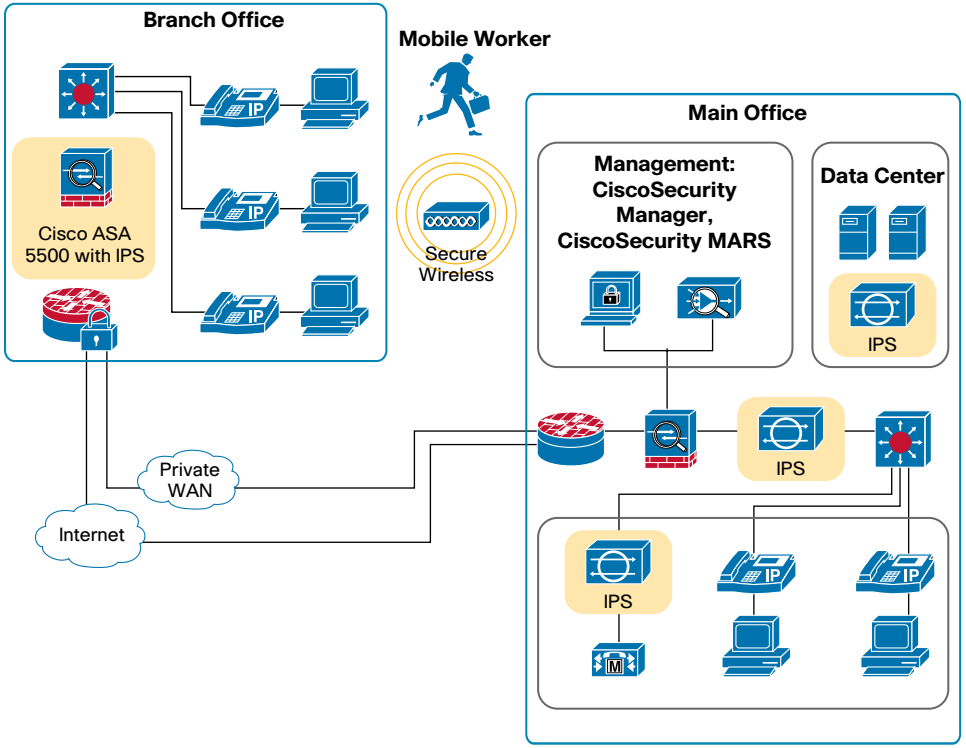
HOME

Overview

The most trusted and widely-deployed IPS in the world, Cisco Intrusion Prevention System (IPS) provides proven protection against over 30,000 threats to help customers secure their confidential data and meet ever-increasing compliance mandates. Cisco IPS accurately identifies, classifies, and stops malicious traffic, including worms, spyware / adware, network viruses, and application abuse before they affect business continuity. Cisco Anomaly Detection stops Day-Zero attacks before signature updates are available.

Cisco IPS collaborates with other key network components for end-to-end network-wide protection. Threat information is shared between Cisco IPS and the host-based IPS Cisco Security Agent and Cisco wireless controller. Available as a dedicated appliance, Cisco IPS is also integrated into Cisco firewall, switch, and router platforms for maximum protection and deployment flexibility.

The following figure shows how Cisco IPS products fit within the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Intrusion Prevention Systems (continued)

HOME

Benefits

- Advanced IPS technology based on 12 years of IPS innovation
- Proven protection against more than 30,000 threats
- Tight integration with host-based IPS (Cisco Security Agent) for end-to-end protection
- Tight integration with Cisco Wireless Controller for secure wireless deployments
- Simplified management with Cisco IPS Manager Express for smaller organizations
- Enterprise-class policy management with Cisco Security Manager and Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)
- Protects against more than just virus outbreaks, such as attacks targeted against a company's information
- Helps prevent against severe loss due to disruptions, theft, or defacement caused by compromised servers
- Stops worm and virus outbreaks at the network level, before they reach the desktop

Flexible deployment options include:

- Cisco IPS 4200 Series Sensors as standalone IPS appliances. Learn more at: http://www.cisco.com/go/4200
- Integrated Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Modules (AIP SSM10, AIP SSM20, and AIP SSM40) provide intrusion prevention, firewall, and VPN in a single, easy-to-deploy platform. Learn more at: http://www.cisco.com/go/aipssm
- Cisco AIM-IPS, NME-IPS, or Cisco IPS Sensor Software for integrated services routers. Learn more at: http://www.cisco.com/go/ime
- Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Modules. Learn more at: http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html
- Cisco Adaptive Wireless IPS protects the wireless signal from being hijacked by an intruder while Cisco's network IPS prevents authenticated users (with a legitimate user name and password) from performing malicious or unauthorized activity, such as stealing confidential data. Learn more at: http://www.cisco.com/go/wips

For more information on Cisco IPS solutions, please visit:
http://www.cisco.com/go/ips

Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Cisco Router Security

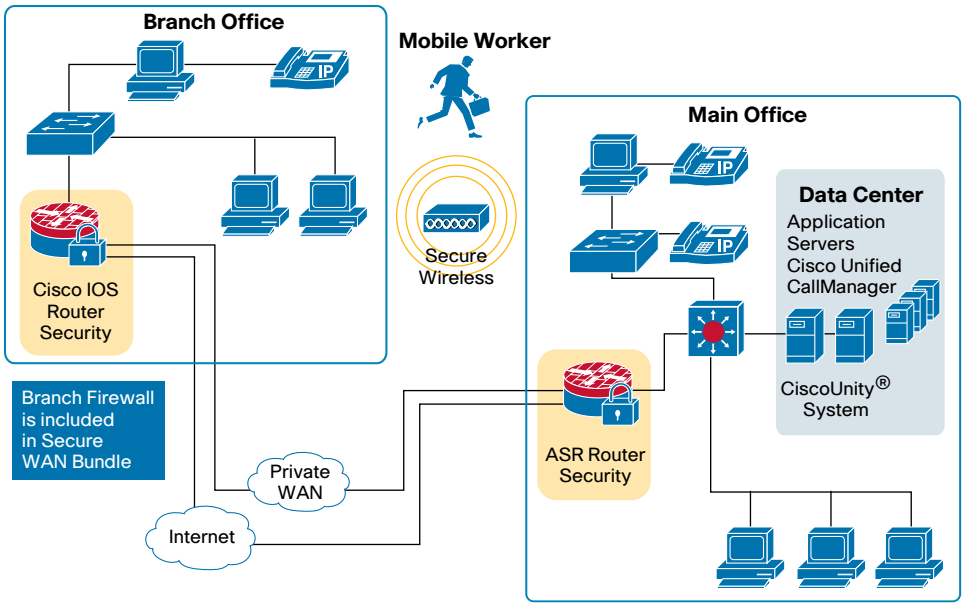
HOME

Overview

It's crucial to secure your critical network infrastructure, including Cisco® routers.

- Cisco Router Security adds important security features with a strong return on investment (ROI).
- This feature set adds the following capabilities to your branch router: site-to-site VPN, IPsec and SSL remote-access VPN, Common Criteria/EAL4-certified stateful firewall, content filtering, inline intrusion prevention, Network Admission Control (NAC), and security management.
- A good business continuity design typically includes encrypted dual WAN links, remote network access during disasters, and stateful failover of critical services. Cisco Router Security enables all these solutions.
- Cisco Router Security can enable other network services such as secure unified communications (voice and video) and secure wireless LAN.

The following figure shows how the Cisco Router Security fits in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Cisco Router Security (continued)

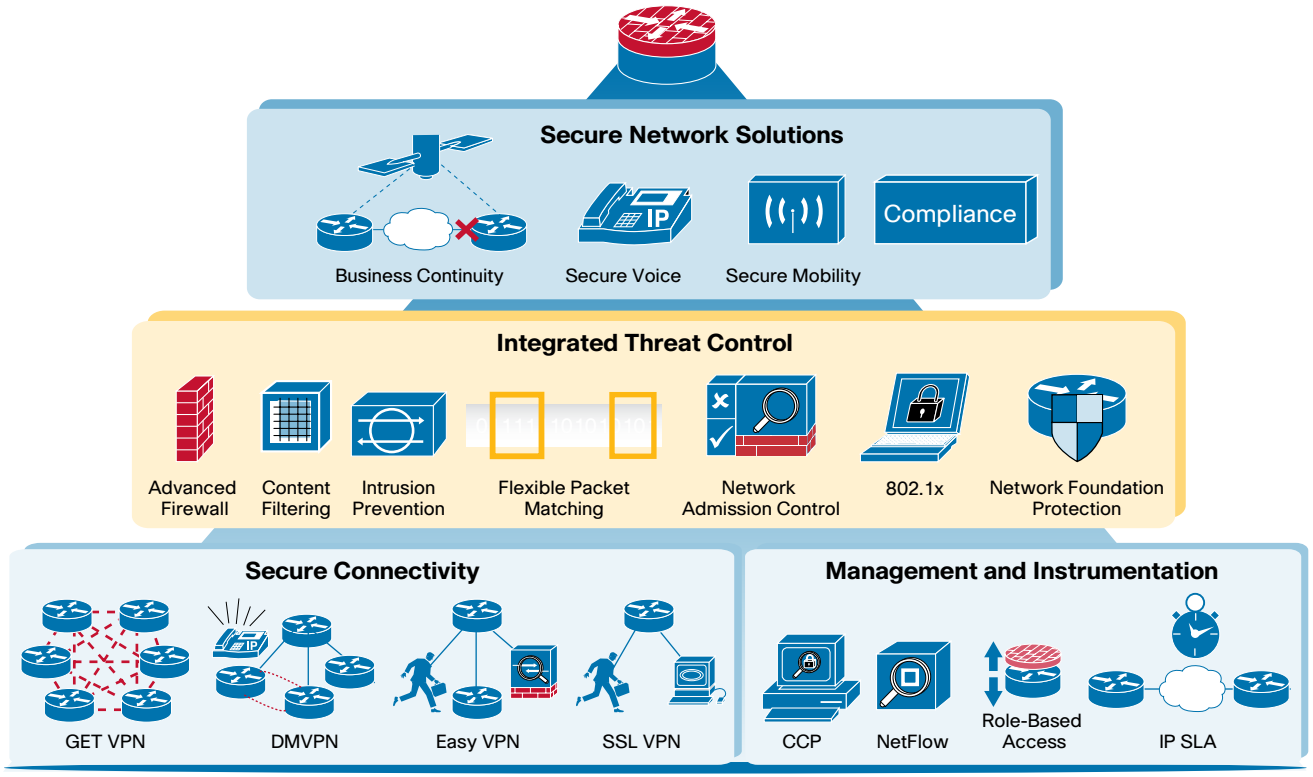
HOME

Benefits

- Maximizes ROI by greatly increasing router value with security services such as firewall, IPsec and SSL VPN, intrusion prevention, content filtering, and Network Admission Control (NAC)
- Enables your business to securely deploy wireless LAN and unified communications services such as voice and video
- Offers a secure, cost-effective, easy-to-manage, and scalable solution for site-to-site business communications
- Enables compliance with U.S. federal and state data and network privacy laws (for example, Payment Card Industry [PCI] requirements)
- Simplifies management burden by converging security and other services in a single network device

For more information, please visit:
http://www.cisco.com/go/routersecurity

The following figure shows the security services available through Cisco Router Security



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Cisco Security Agent

Overview

Cisco® Security Agent is the first endpoint security solution that combines zero-update attack protection, data loss prevention, and signature-based antivirus in a single agent. This unique blend of capabilities defends servers and desktops against sophisticated zero-day attacks, and enforces acceptable-use and compliance policies within a simple management infrastructure.

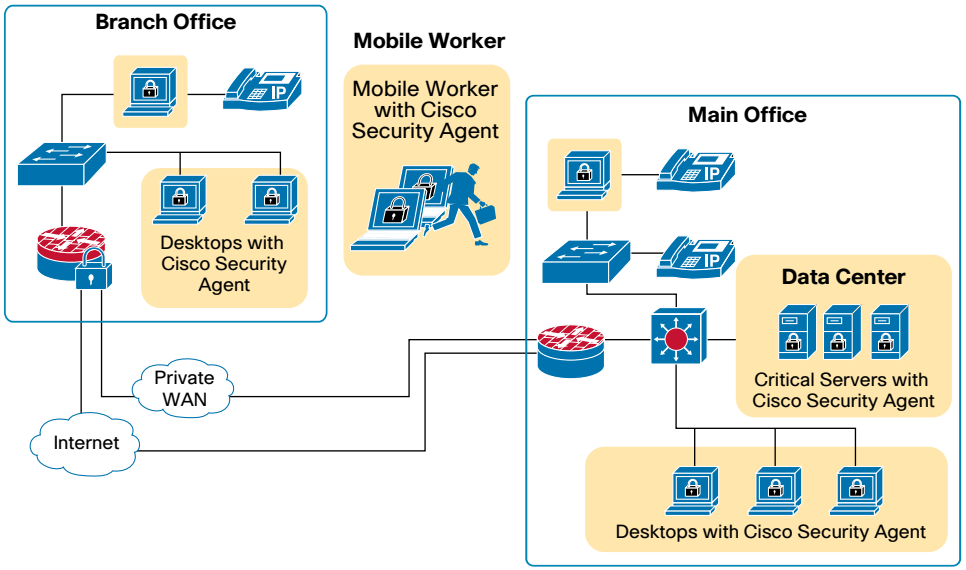
- You will save on your security budget with better security: Cisco Security Agent 6.0 includes antivirus at no additional cost and no charge for renewals.
- Data loss prevention is integrated with Cisco Security Agent endpoint security: A single agent and single management console protects both the integrity of the endpoint and confidential data.
- Cisco Security Agent provides certified PCI protection.
- Cisco Security Agent is the industry leader in defending endpoints against targeted attacks, malicious mobile code, rootkits, worms, and zero-day attacks.

Benefits

- Zero-update protection reduces emergency patching in response to vulnerability announcements, minimizing patch-related downtime and IT expenses.
- Visibility and control of sensitive data protects against loss from both user actions and targeted malware.
- Predefined compliance and acceptable use policies allow for efficient management, reporting, and auditing of activities.
- "Always-vigilant" security means that your system is always protected, even when users are not connected to the corporate network or lack the latest patches.

For more information, please visit:
http://www.cisco.com/go/csa

The following figure shows how Cisco Security Agent fits in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

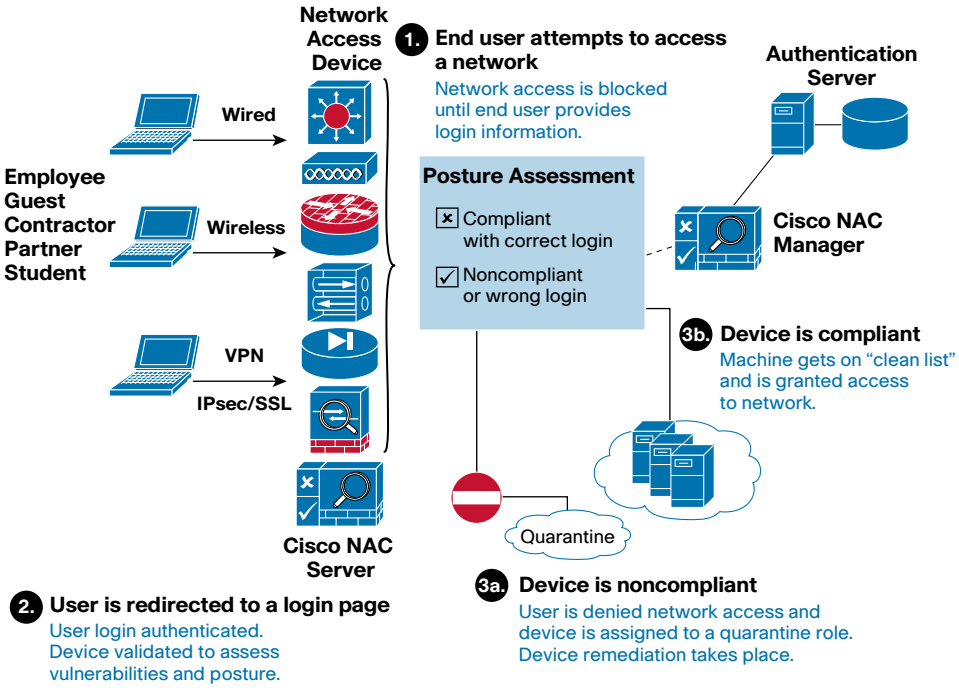
EXIT

Cisco Network Admission Control

Overview

- Cisco® Network Admission Control (NAC) enables the network to enforce security policies on all devices seeking to access the network.
- Cisco NAC protects sensitive data and prevents unauthorized access by confirming a user's identity before access to the network is granted.
- Cisco NAC minimizes the risks associated with noncompliant devices, regardless of system type, ownership, or access methods, resulting in more resilient and secure networks.
- Noncompliant devices can be quarantined and brought into compliance.
- The optional Cisco NAC Profiler automates discovery and inventory of all LAN-attached endpoints, including non-PC devices such as IP phones and printers. It simplifies NAC deployment by using the device information to apply appropriate Cisco NAC policies.
- The optional Cisco NAC Guest Server supports the entire guest access lifecycle (provisioning, notification, management, and reporting).

The following figure shows how Cisco NAC fits in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Cisco Network Admission Control
(continued)

Benefits

- Enforces security policy compliance at the network level
- Proactively protects against infrastructure disruptions (such as viruses and worms)
  - Controls and reduces large-scale infrastructure disruptions
  - Reduces operating expenses and maintains higher employee productivity
- Prevents unauthorized access
  - Controls network access based on user and device credentials to maintain security and protect confidential information
  - Provides effective controls for guest access and partner connections
- Provides complete services (user authentication, device posture validation, policy enforcement, remediation, device profiling, and secure guest) to meet customer business needs
- Profiling service reduces IT burden by automating device discovery and inventory
- Guest service provides secure guest access and guest satisfaction
- Supports all use cases, including campus, branch offices, wireless, and VPN
- Secures both company-owned and non-company-owned devices
- Can be deployed for Layer 2 or Layer 3, in-band or out-of-band
- Reduces IT security risks and addresses compliance requirements

For more information, please visit:
http://www.cisco.com/go/nac

Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

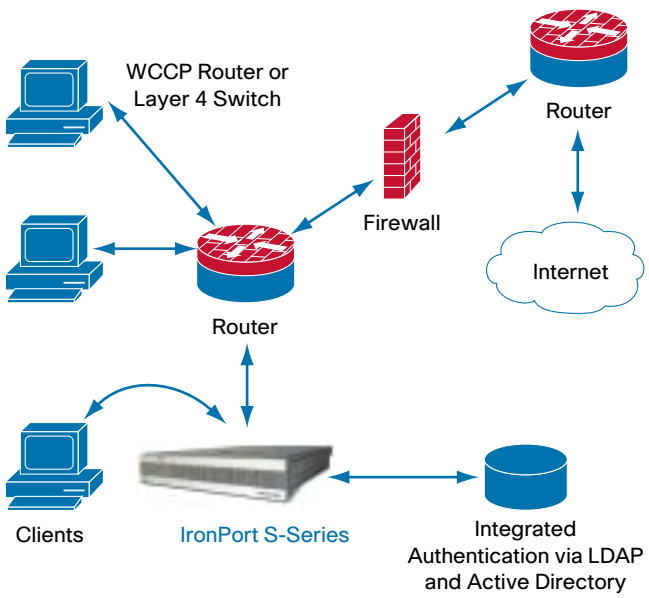
Cisco Web Security Gateway Appliances

Overview

The number of security threats introduced by web traffic has reached epidemic proportions. Traditional gateway defenses are proving to be inadequate against a variety of web-based malware, leaving corporate networks exposed to the inherent danger posed by these threats.

- According to industry estimates, approximately 75 percent of corporate PCs are infected with spyware, yet less than 10 percent of corporations have deployed perimeter malware defenses.
- The Cisco® IronPort® S-Series Web Security Gateway Appliance is the industry's first and only appliance to combine traditional URL filtering, reputation filtering, and malware filtering on a single platform.
- The S-Series provides multiple layers of defense on a single appliance while maintaining carrier-class performance.

The following figure shows how the Cisco IronPort S-Series fits in the network.



Benefits

- The Cisco IronPort S-Series offers a single-appliance solution to secure and control the three greatest web traffic risks facing enterprise networks: security risks, resource risks, and compliance risks.
- By stopping malware threats at the network perimeter with the Cisco IronPort S-Series, enterprises can significantly reduce administrative costs, prevent attacker "phonehome" activity on networks, reduce support calls, enhance worker productivity, and eliminate the business exposure that accompanies these threats.
- The industry's first web reputation filters provide a powerful outer layer of defense. Cisco IronPort Web Reputation Filters use SenderBase technology to analyze more than 50 different web traffic and network-related parameters to accurately evaluate a URL's trustworthiness.
- By implementing acceptable use policies, enterprises can not only monitor activities, but can also help generate awareness and increase education about the risks these policies help mitigate.
- Unlike other ICAP-based solutions that require multiple pieces of hardware to maintain, the Cisco IronPort S-Series provides a single platform that contains a complete, in-depth defense.
- Designed to minimize administrative overhead, Cisco IronPort S-Series appliances offer easy setup and management with an intuitive graphical user interface, support for automated updates, and comprehensive monitoring and alerting.
- Cisco IronPort S-Series appliances deliver real-time and historical security information, enabling administrators to quickly understand web traffic activity.

For more information, please visit:
http:// www.ironport.com/web

Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Cisco IronPort Email Security Appliances

Overview

Cisco provides the world's most powerful multilayered approach to email security. The Cisco® IronPort® C-Series provides world-class spam protection, data loss prevention, preventive virus outbreak filters, and signature-based reactive filters, combined with content filtering and best-of-breed encryption technology, to deliver the highest level of email security available today.

Today's email-borne threats consist of virus attacks, spam, false positives, distributed denial-of-service (DDoS) attacks, spyware, phishing (fraud), regulatory compliance violations, and data loss. The unparalleled performance of the Cisco IronPort email security appliance delivers industry-leading protection from inbound spam and virus attacks and outbound data loss possibilities, in an easy-to-use appliance.

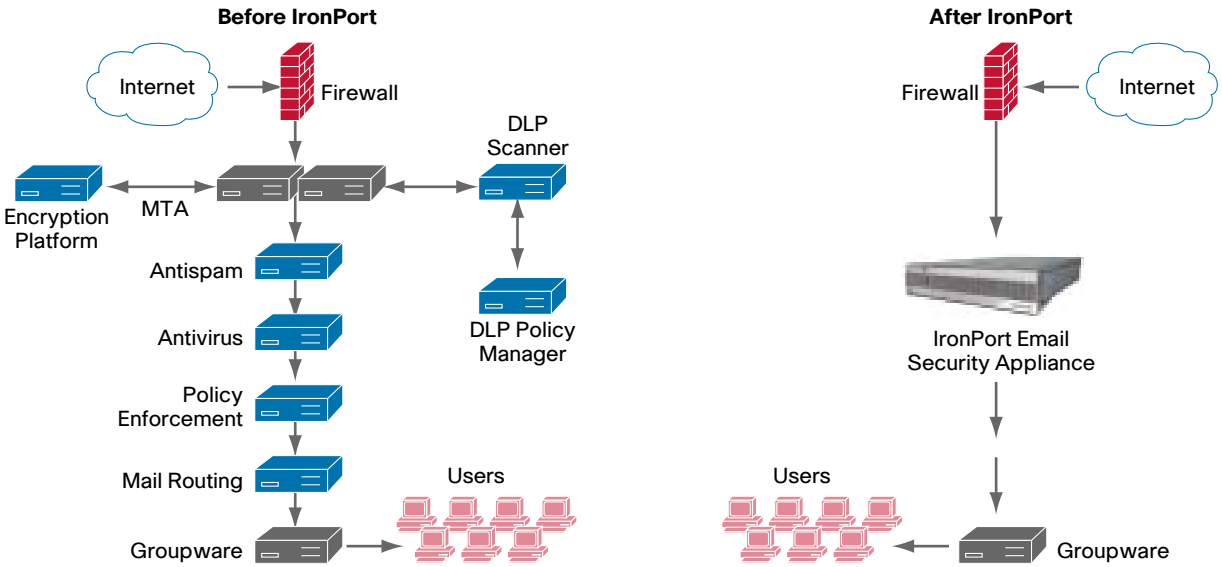
Benefits

Cisco IronPort's antispam solutions quickly and accurately protect customers from spam outbreaks.

- Cisco IronPort combines SenderBase Reputation Filters with content-level analysis and Cisco IronPort Anti-Spam, to protect customers from an industry best: removing 99% of spam with near-zero false positives.
- The Cisco IronPort C-Series enables a significant reduction in TCO by consolidating email operations and security into a single platform. The unparalleled performance of the C-Series delivers dial-tone availability—saving hours of productivity and thousands of dollars during peak traffic times.
- Cisco IronPort provides system administrators with the necessary information to make critical security decisions and demonstrate ROI.

For more information, please visit:
http:// www.ironport.com/email

The following figure shows how Cisco IronPort fits in your network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Cisco ACE Web Application Firewall

Overview

Many organizations are looking to increase efficiency and profitability through new Web 2.0 applications and services. Unfortunately, these new applications are often customized and poorly secured.

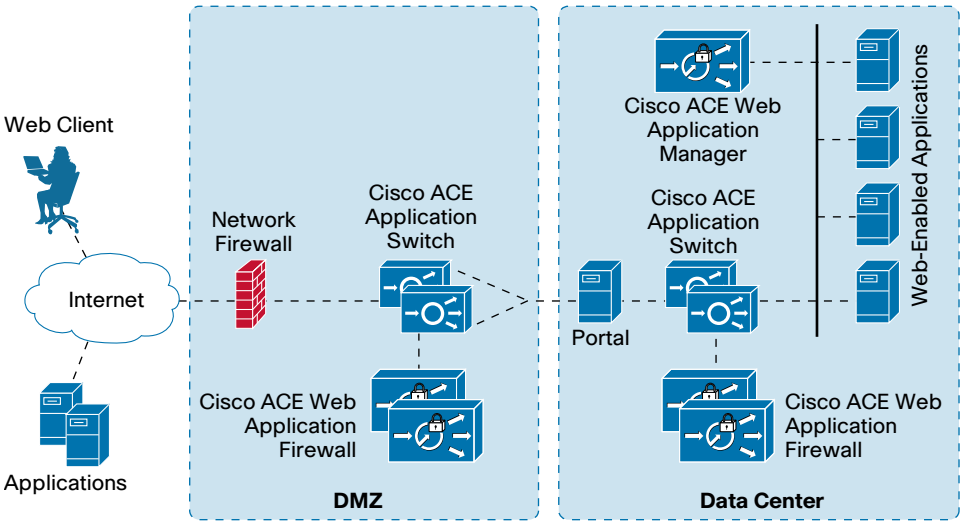
- The Cisco® ACE Web Application Firewall combines deep web application analysis with high-performance Extensible Markup Language (XML) inspection and management to address the full range of threats to web applications, including identity theft, data theft, information leakage, application disruption, fraud, and targeted attacks.
- The Cisco ACE Web Application Firewall is especially designed to help organizations that store, process, and transmit credit card data to comply with the current Payment Card Industry (PCI) Data Security Standard (DSS) requirements.
- Because of its unique blend of HTML and XML security, the Cisco ACE Web Application Firewall provides a full compliance solution for PCI DSS sections 6.5 and 6.6, which mandate the implementation of a web application firewall.

Benefits

- PCI DSS regulation compliance, with out-of-the-box customizable PCI policies and securing, auditing, and reporting on web application activity
- Full-proxy security for both traditional HTML-based web applications and modern XML-enabled web services applications
- Authentication and authorization enforcement to block unauthorized access
- Best-in-industry scalability throughput for managing XML application traffic in largest of data centers
- Positive and negative security enforcement to keep bad traffic patterns out and identify and allow only good traffic through
- Enterprisewide, user-friendly management accessible anywhere on the network through the web GUI

For more information, please visit:
http://www.cisco.com/go/waf

The following figure shows how a Cisco ACE Web Application Firewall fits in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

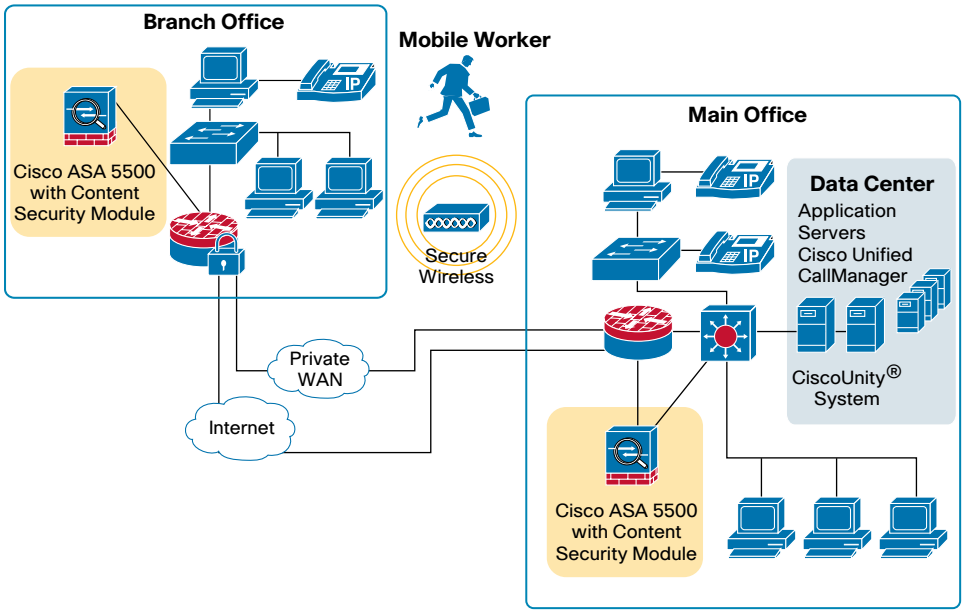
EXIT

Content Security on the Cisco ASA 5500 Series

Overview

- The Cisco® ASA 5500 Series Adaptive Security Appliance with the Content Security and Control Security Services Module (CSC-SSM) is an all-in-one threat defense appliance that takes advantage of Cisco's leadership in firewall and VPN technology and Trend Micro's expertise in antimalware and gateway content security.
- The Cisco ASA 5500 Series with CSC-SSM allows network and security administrators to accurately identify, classify, and stop malicious traffic, including worms, spyware/adware, network viruses, and application abuse, before they affect business continuity.
- Filtering content at the gateway provides a consistent layer of content protection for company-owned and guest computers, regardless of the type or status of antivirus protection on those computers. The CSC-SSM provides a comprehensive set of content security services, including antispam, URL filtering and blocking, antiphishing, and antispyware, in addition to antivirus services.

The following figure shows how Cisco content security solutions fit in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Content Security on the Cisco ASA 5500 Series (continued)

Benefits

- The Cisco ASA 5500 Series with the CSC-SSM is an all-in-one appliance that includes firewall and VPN security, and interoperates well with the Cisco VPN concentrators and Cisco PIX® firewalls that are still deployed in some remote offices.
- The all-in-one appliance minimizes day-to-day management while improving operational efficiency compared with separate solutions.
- Firewall and VPN security are complemented with URL and email filtering and protection from viruses, spam, spyware, and phishing.
- Full-featured, in-depth, and convenient, the CSC-SSM include antivirus, antispam, antiphishing, antispyware, and URL and email filters.
- The CSC-SSM includes configurable spam filters. Email reputation provides real-time information about senders of spam and botnets by assigning a reputation score to their IP addresses. Email from suspect IP addresses can then be blocked automatically "in the cloud," before the messages reach the company's network. This level of domain customization increases the control that organizations have over their email traffic and helps conserve bandwidth on internal networks.
- Gateway, desktops, servers, and email are protected, 90 percent of spam is blocked, and traffic to and from disreputable sites is blocked.
- Unwanted content does not clutter the network or system. Bandwidth and storage are not flooded with spam.
- The CSC-SSM solution is low-maintenance—updates and filtering are carried out automatically once setup is complete.

For more information, please visit:
http://www.cisco.com/go/cscssm

Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

Cisco Security Monitoring, Analysis, and Response System

Overview

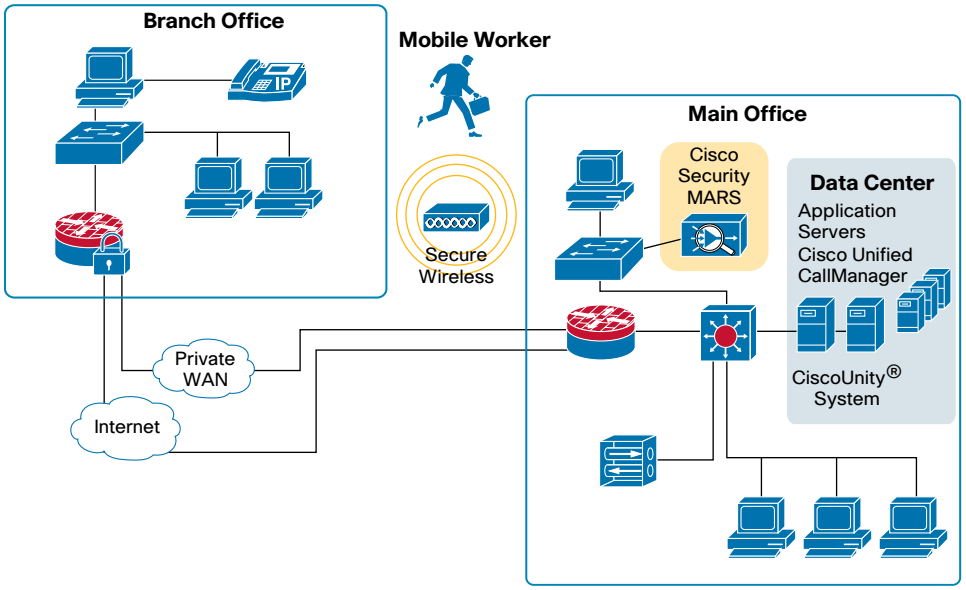
- The Cisco® Security Monitoring, Analysis, and Response System (Cisco Security MARS) is a family of high-performance, scalable appliances for threat management, monitoring, and mitigation. Cisco Security MARS helps customers achieve greater security and make more effective use of network and security devices.
- Cisco Security MARS combines traditional security event monitoring with network intelligence to deliver precise mitigation intelligence for real-time response to attacks, intrusions, and other network threats.

Benefits

- Collects, analyzes, and correlates data from a diverse set of Cisco devices
- Shows a graphical attack path using topology awareness
- Suggests mitigation for rapid threat containment
- Links with Cisco Security Manager for policy provisioning and event lookup
- Optimized for Cisco ASA and Cisco IPS troubleshooting
- Delivers high performance: A single Cisco Security MARS appliance can handle up to 15,000 events per second

For more information, please visit:
http://www.cisco.com/go/mars

The following figure shows how Cisco Security MARS fits in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Cisco Security Manager

Overview

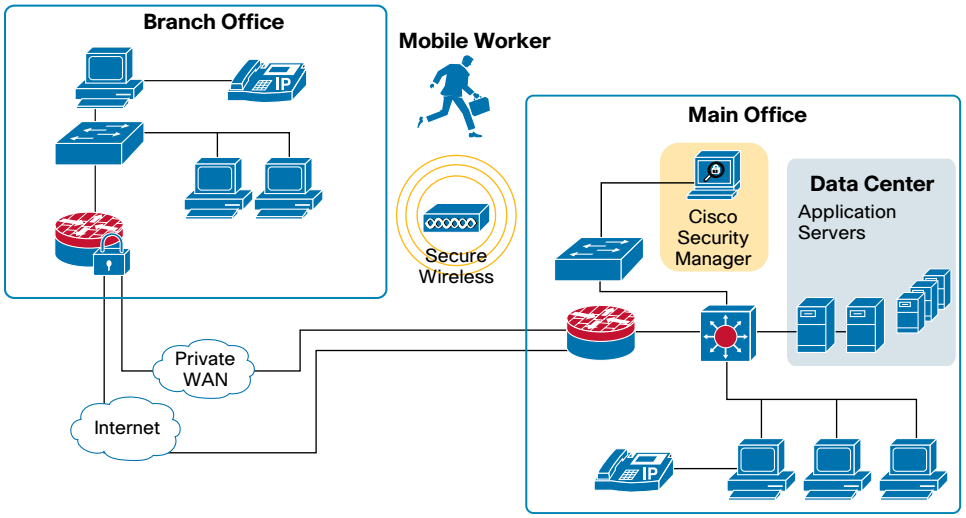
- Cisco® Security Manager is a powerful but easy-to-use solution that centrally provisions all aspects of device configurations and security policies for Cisco firewalls, VPNs, and intrusion prevention systems (IPSs).
- Cisco Security Manager provides centralized security administration, faster deployment, and increased configuration accuracy.
- The solution is effective for managing small networks consisting of fewer than 10 devices, but also scales to efficiently manage large-scale networks composed of thousands of devices.

Benefits

- Provides a single integrated application for managing firewall, VPN, and IPS security services on Cisco security appliances and modules, routers, and switches
- Reduces operational expenses while improving provisioning accuracy and consistency
- Collaborates with Cisco Security MARS to form a comprehensive security management solution that encompasses security provisioning, event monitoring, threat detection, and mitigation
- Allows faster response to threats—Defines and assigns new security policies to thousands of devices in a few simple steps
- Provides superior ease of use with a rich graphical user interface
- Supports true enterprise-class operational environments with support for multiple simultaneous security administrators with fine-grained control of access permissions; an optional "workflow" mode allows the security and network operations staff to work together effectively with the appropriate division of responsibilities
- Supports provisioning for Cisco router, switch, and security platforms

For more information, please visit:
http://www.cisco.com/en/US/products/ps6498/index.html

The following figure shows how Cisco Security Manager fits in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Cisco Secure Access Control System

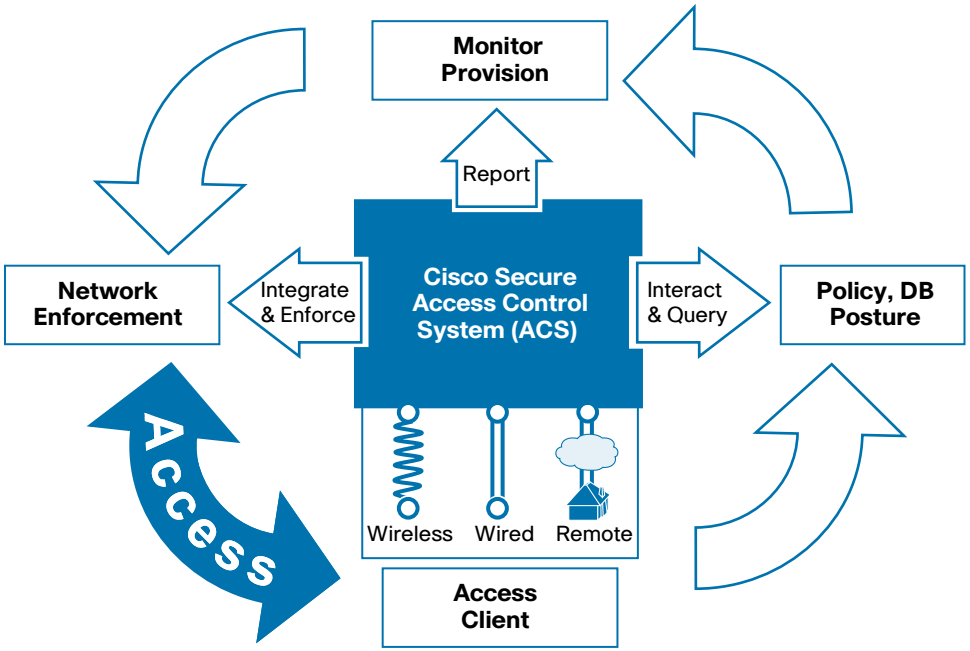
Overview

- Cisco® Secure ACS is the world's most-trusted enterprise network access policy and identity system, used by more than 40,000 enterprises worldwide.
- With powerful performance and a design-for-versatility approach, Cisco Secure ACS provides a crucial building block for almost any network identity and access policy strategy.
- Cisco Secure ACS interacts with external databases, policy servers, and posture engines, becoming a control point for managing network access policy.
- Cisco Secure ACS provides better control, monitoring, and enforcement of access to corporate resources to meet ever-changing business and regulatory needs.

Benefits

- Centralized control for network access and device administration.
- Can be used with virtually any network device that supports RADIUS or TACACS+.
- Built to meet the needs of large networked environments with support for redundant servers, remote databases, database replication, and backup services.
- For the small enterprise and SMB, Cisco Secure ACS Express provides a powerful yet economical package.
- Cisco Secure ACS View provides enhanced reporting, monitoring, and troubleshooting designed for the highest levels of visibility, control, and compliance.

For more information, please visit:
http://www.cisco.com/go/acs



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Cisco Enterprise Policy Manager

Overview

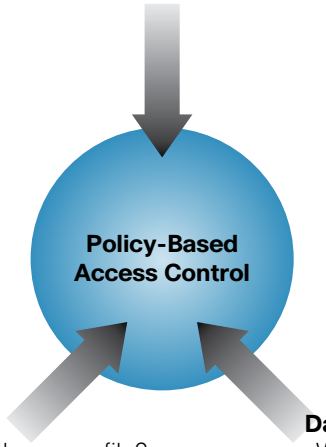
- Cisco® Enterprise Policy Manager is the market-leading policy-based authorization solution for enterprise applications and data, providing fine-grained and differentiated access control.
- Cisco Enterprise Policy Manager externalizes the policy decision services from existing applications, collaboration services, and network infrastructure.
- Cisco Enterprise Policy Manager allows companies to extract business logic that makes access policy decisions from individual applications. This looser binding of policy from application logic makes it easier (and much faster) to respond to changing regulations and business needs.
- Cisco Enterprise Policy Manager is a component of Cisco's Service-Oriented Network Architecture (SONA) strategy with the network becoming the provider of policy services to service-oriented architecture (SOA), Web 2.0, collaboration, unified communications, and enterprise applications.

Benefits

- Consistent administration and enforcement of entitlement policies ("configure not code"):
  - Centralized, delegated management is usable by non-developers
  - Consistently applied for local and remotely hosted resources
- Centralized auditing and real-time remediation:
  - Policy what-ifs
  - Comprehensive "who has access to what, and, who accessed what"
- Enterprise-class, standards-compliant product with out-of-the-box integration with existing customer infrastructure
- Scalable from single application, to heterogeneous LoB, to globally distributed enterprise

For more information, please visit:
http://www.cisco.com/go/epm

Reachability
- Is Joe (who is an HR admin) allowed to access an HR application from an "un-trusted" network?



Functional
- Is Joe allowed to view employee profile?
- Can he adjust salary (if so, what limit/approval)?

Data
- What fields of the employee profile can Joe see?
- Is he entitled to view address of employees in "EMEA" and can he see data about all VPs and their direct reports?

Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Switch Security

HOME

Cisco Catalyst 6500 Series Security Services Modules

Overview

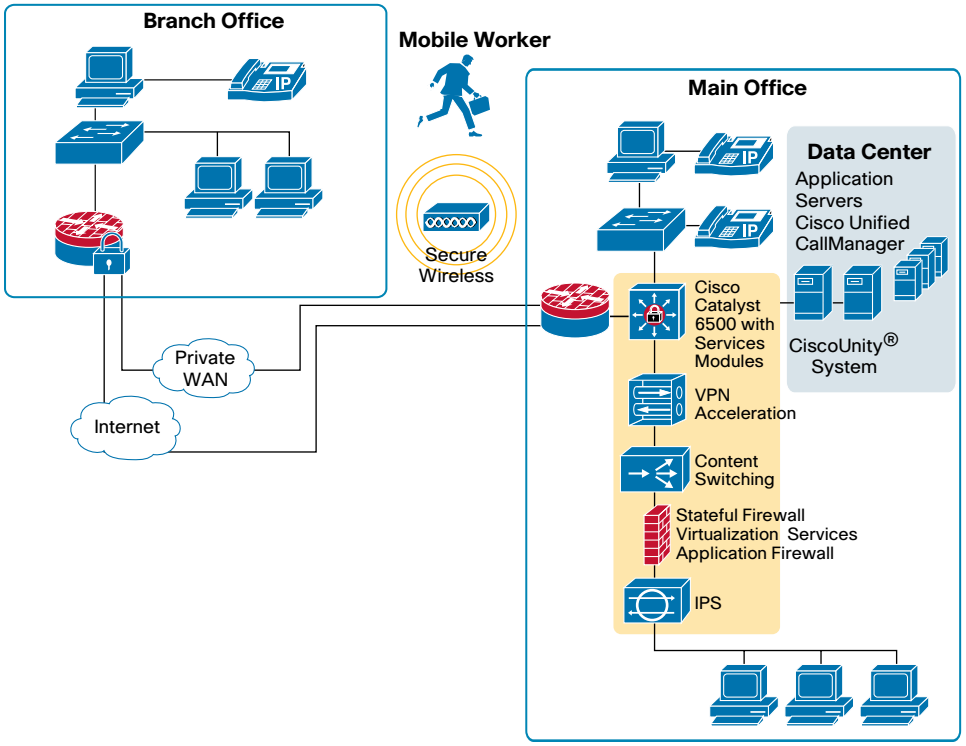
- Cisco delivers integrated network security with a suite of advanced security modules for Cisco® Catalyst® 6500 Series Switches. These include firewall, intrusion prevention system (IPS), IP Security (IPsec) VPN, Secure Sockets Layer (SSL) acceleration, distributed denial-of-service (DDoS), and content switching modules.
- These security modules enable integrated, highly available, adaptive, and scalable security for network connectivity, services, and applications.

Benefits

- Ability to increase security while using existing Cisco Catalyst 6500 Series investment
- Tightly integrated infrastructure security solutions
- Highest-performance security solutions, offering multigigabit performance in a single Cisco Catalyst 6500 Series Switch
- Application-level visibility into the infrastructure
- Critical platform for collaboration of emerging technologies (such as applicationnetworking)

For more information, please visit:
http://www.cisco.com/go/switchsecurity

The following figure shows how Cisco Catalyst 6500 Series Security Services Modules fit in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Switch Security

HOME

Cisco TrustSec

Overview

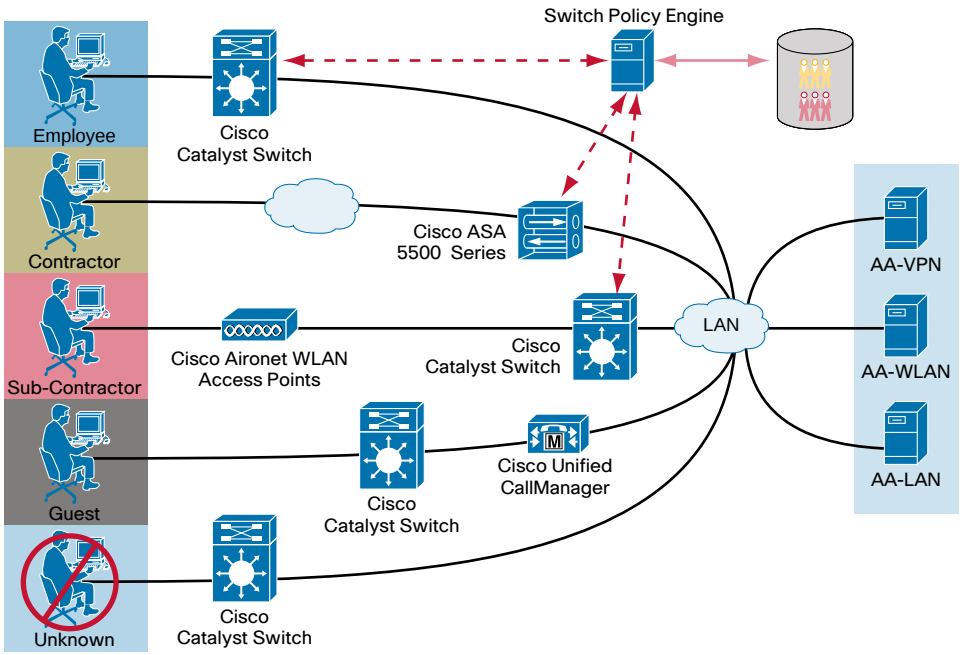
- Cisco® TrustSec provides secure campus access control. It protects customer data and resources by controlling access based on a user's role in the organization. It works independent of how users connect to your network, when they connect, and where they connect.
- Cisco TrustSec enables a converged policy framework. TrustSec helps customers consolidate multiple access policies into a centralized policy framework for consistency and scalability. TrustSec can also act as a broker between the campus network infrastructure and back-end policy directories such as Active Directory.
- Cisco TrustSec delivers pervasive integrity and confidentiality protection. TrustSec safeguards sensitive data and defeats man-in-the-middle attacks by providing switch-level hop-to-hop encryption between switch ports.

Benefits

- Provides consistent role-based identity and controlled access to critical applications and resources
- Converges various roles, servers, and access definitions into a centralized policy framework and simplifies identity-based policy management
- Safeguards against data loss in support of regulatory requirements
- Collaborates with Cisco Identity-Based Networking Services (IBNS) to provide flexible authentication and policy controls
- Enables scalable switch security services
- Streamlines policy management and implementation, allows new business opportunities, improves security, reduces IT total cost, and helps achieve regulatory compliance

For more information, please visit:
http://www.cisco.com/go/trustsec

The following figure shows how Cisco TrustSec fits in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

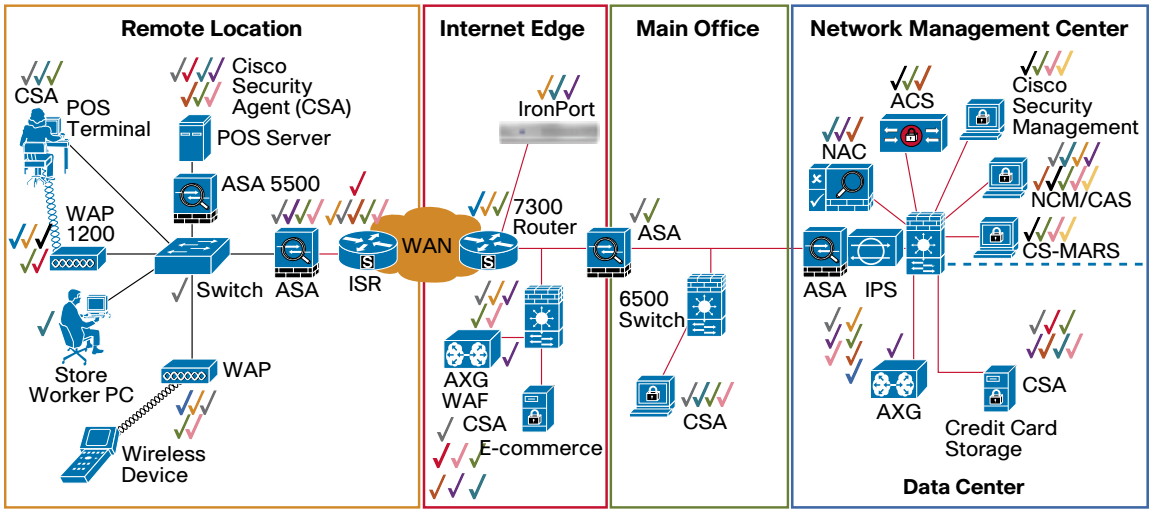
Putting It All Together

EXIT

Compliance

Overview

- The Payment Card Industry (PCI) is a global industry standard to protect customer credit card information while it is in process, in transit, or while being stored.
- Cisco® PCI Validated Architectures, a set of architectures audited by a PCI Qualified Security Assessor (QSA) address many of the PCI requirements.
- The Cisco PCI solution includes Cisco products and services:
  - Cisco ASA 5500 Series Adaptive Security Appliances with firewall, VPN, and IPS
  - Cisco IOS® Software on Cisco integrated service routers with firewall, VPN, and IPS
  - Unified Wireless Network with Cisco Wireless Control Server (WCS), Wireless LAN Controller, and Aironet® 1100 and 1200 Series Wireless Access Points
  - Cisco Security Agent
  - Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS)
  - Cisco Security Manager
  - CiscoWorks Network Compliance Manager
  - Cisco Network Admission Control (NAC) Appliance
  - Cisco IronPort® Email Security
  - Cisco ACE WAF
  - Cisco IPS 4200 Series intrusion prevention system appliances
  - Cisco Catalyst® 6500 Series Firewall Services Module (FWSM) and Intrusion Detection Services Module (IDSM-2)
  - Cisco Secure Access Control System (ACS)
  - Professional services that can help achieve PCI compliance, and then help maintain a compliant state
- Cisco PCI Services from Cisco and from Cisco Security Specialized Partners include:
  - Cisco PCI Gap Analysis Service
  - Cisco PCI Remediation Service
  - Cisco PCI Remote Monitoring and Management Service
  - Cisco PCI Periodic Gap Analysis Service



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Compliance
(continued)

Benefits

- Reduces network complexity, expense, and risk of fines and penalties by establishing a proven, PCI-validated architecture
- Provides organizations with a step-by-step approach toward achieving PCI compliance
- Shows how customers can use their existing Cisco investment
- User-friendly and auditor-friendly PCI reports reduce audit time and expense
- End-to-end integrated solution delivers stronger value beyond individual product benefits

For more information, please visit:
http://www.cisco.com/go/compliance

Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

Cisco Virtual Office

Overview

The adoption of teleworking is increasing due to globalization, rising fuel and energy prices, "green" initiatives, and the increase in collaboration applications for business communications. Cisco® Virtual Office:

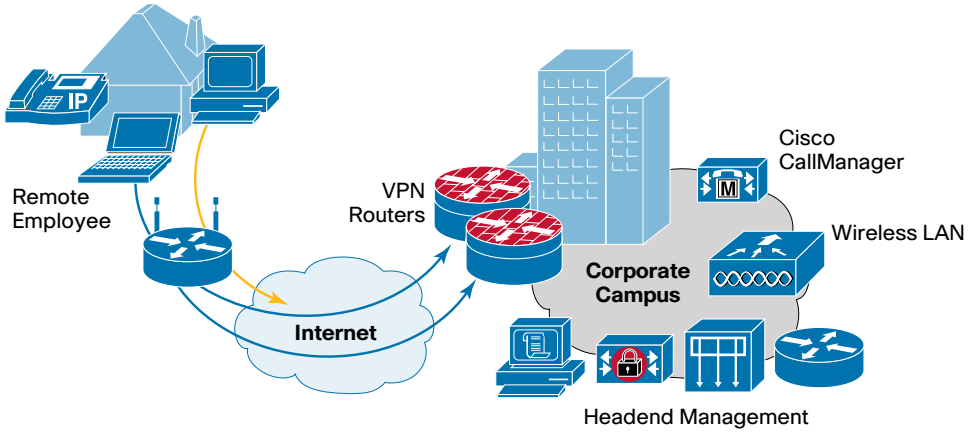
- Enables businesses to extend their enterprise to the remote workforce by providing data, voice, video, and wireless mobility services in a centrally managed environment
- Addresses the security requirements of remote workers by providing dedicated VPN, firewall, IPS, and content security features on the integrated services router platform.
- Provides a seamless experience for remote workers and teleworkers by providing the same IT services that employees expect in a traditional corporate environment.

The Cisco Virtual Office architecture is ideal for home offices, small branch offices, call centers, and mobile business partners and contractors.

The following figure shows a Cisco Virtual Office deployment for a home office user.

The Network Enables:

- Office-caliber data, voice, and video services
- Integrated security extended to the remote user
- Scalable, low-cost VPN architecture



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Cisco Virtual Office
(continued)

Benefits for Employees

- Increased schedule flexibility for improved work-life balance
- Reduced costs and commute time
- Improved reliability and access to collaboration tools for better productivity
- Ease of use and setup

Benefits for the Company

- Consistent security policy enforcement for better risk mitigation
- Ease of management and the ability to scale IT
- Continuity of operations and business agility
- Cost savings associated with real estate, energy, and operations
- Talent attraction and retention

For more information, please visit:
http://www.cisco.com/go/cvo

Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

Site-to-Site VPNs

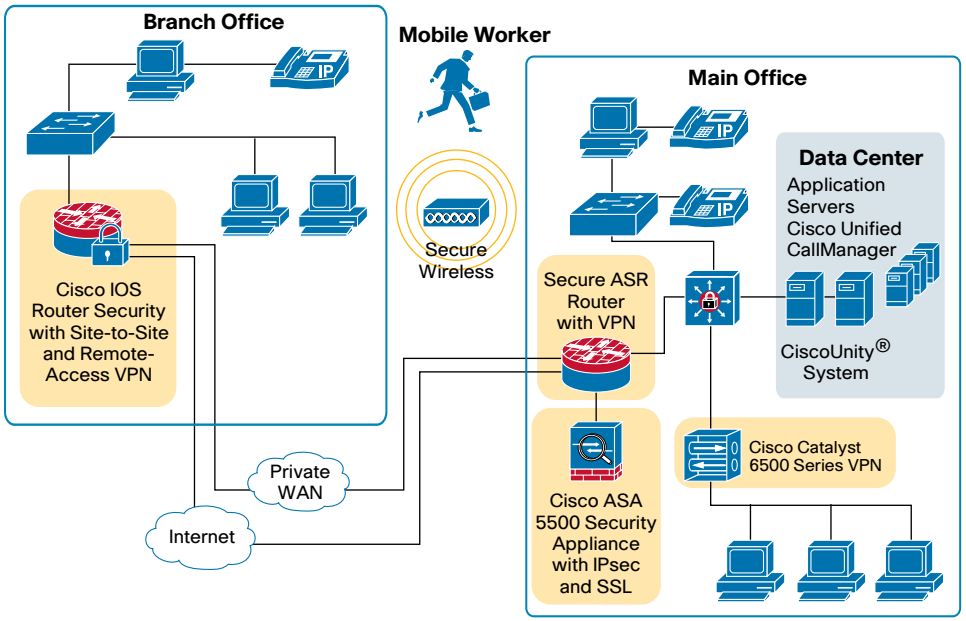
Overview

VPNs enable the deployment of fast, reliable, and secure connectivity for remote offices, business partner locations, and other branch sites. The data, voice, and video communications between these locations are kept confidential across untrusted networks. Cisco offers a variety of VPN solutions that provide cost-effective and highly manageable secure connectivity.

Cisco offers multiple VPN technologies, including IPsec VPN, Dynamic Multipoint VPN (DMVPN), and Group Encrypted Transport VPN (GET VPN), integrated on a single platform, reducing equipment cost and management complexity. Collectively, these solutions represent the most comprehensive and scalable VPN portfolio in the industry.

- Cisco® VPN solutions provide integrated, threat-protected VPN features that guard against malware and hackers without the cost and complexity of deploying additional security equipment.
- Cisco VPN solutions include:
  - Cisco routers: Cisco's most advanced site-to-site VPN solution plus integrated remote-access, firewall, intrusion prevention system (IPS), and content security services
  - Cisco ASA 5500 Series: Cisco's most advanced remote-access VPN solution, delivering integrated site-to-site VPN, remote-access VPN, firewall, IPS, and content security services
  - Cisco Catalyst® 6500 Series: Cisco's most scalable VPN platform plus integrated firewall and IPS services

The following figure shows how Cisco site-to-site VPNs fit in the network



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Site-to-Site VPNs
(continued)

Benefits

- Site-to-site VPNs securely connect office locations utilizing the Internet to decrease costs and increase flexibility.
- Support for multiple VPN technologies from a single platform reduces cost and complexity while enabling VPN services that are customized for the deployment environment.
- Fully network-aware VPNs deliver any application, including voice and video, to any location with a high level of integrity.
- Integrated threat-protection VPN services defend network threats without the need for additional security equipment.

For more information, please visit:
http://www.cisco.com/go/vpn

Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

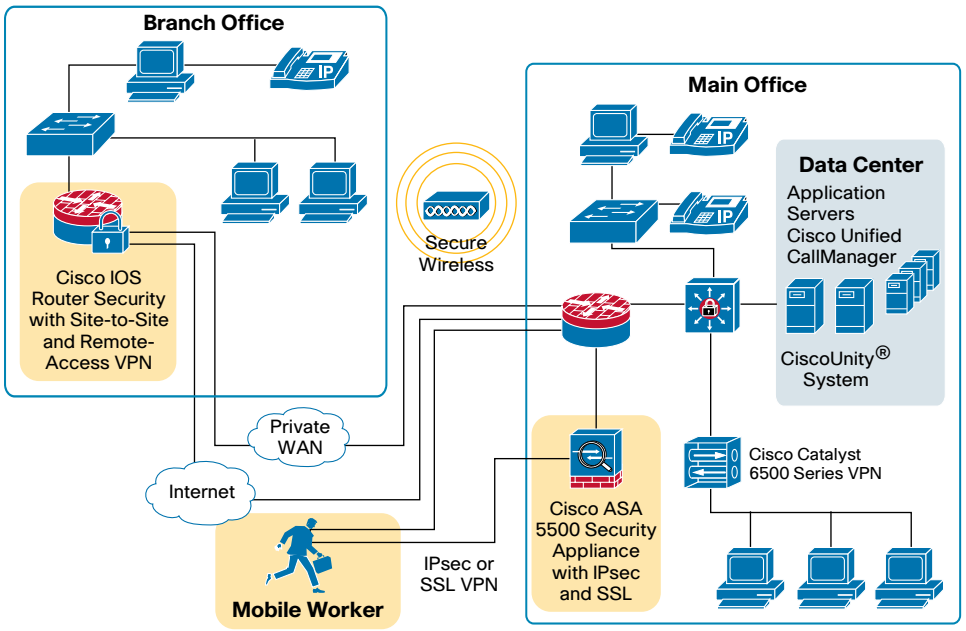
Putting It All Together

Remote-Access VPNs

Overview

- Remote-access VPNs enable fast, reliable, and secure connectivity to the corporate network from practically anywhere, anytime, with any device. They allow secure remote access to the corporate network based on user roles, whether they are remote workers, employees, contractors, or business partners. Cisco offers a variety of VPN solutions, including IP Security (IPsec) and Secure Sockets Layer (SSL) VPN, that provide cost-effective and highly manageable remote connectivity.
- Cisco® VPN technologies are integrated on a single platform, reducing equipment cost and management complexity. Collectively, these solutions represent the most comprehensive and scalable VPN portfolio in the industry.
- Cisco VPN solutions provide integrated threat protection that guards against malware and hackers without the cost and complexity of deploying additional security equipment.
- Cisco VPN solutions include:
  - Cisco ASA 5500 Series: Cisco's most advanced remote-access VPN solution, which delivers concurrent user scalability from 10 to 10,000 sessions, plus integrated site-to-site VPN, firewall, intrusion prevention system (IPS), and content security services
  - Cisco routers: Cisco's most advanced site-to-site VPN solution plus integrated remote-access, firewall, and IPS services
  - Cisco Catalyst® 6500 Series: Cisco's most scalable VPN platform plus integrated firewall and IPS services

The following figure shows how Cisco remote-access VPNs fit in the network.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT

Remote-Access VPNs
(continued)

Benefits

- Remote-access VPNs increase productivity by extending secure network access for remote workers, anytime, anywhere, and with any type of device, including PDAs, smartphones, public kiosks, personal laptops, and shared computers. Access can be customized according to user roles, such as “day-extenders,” full-time employees, remote workers, contractors, or business partners.
- Remote-access VPNs simultaneously support IPsec (remote-access and site-to-site) and SSL VPN connectivity from a single platform, reducing cost, complexity, and management overhead while enabling VPN services customized for the deployment environment.
- Remote-access VPNs support IPsec and clientless SSL VPN.
- Fully network-aware VPNs deliver any application, including voice and video, to any location with a high level of integrity.
- Integrated threat-protection services defend against viruses, spyware, and hackers traversing the VPN connection, without the need for additional security equipment.
- Clientless SSL VPNs provide simplified administration by enabling remote-access connectivity through any Internet-enabled location with a standard web browser.

For more information, please visit:
http://www.cisco.com/go/sslvpn

Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

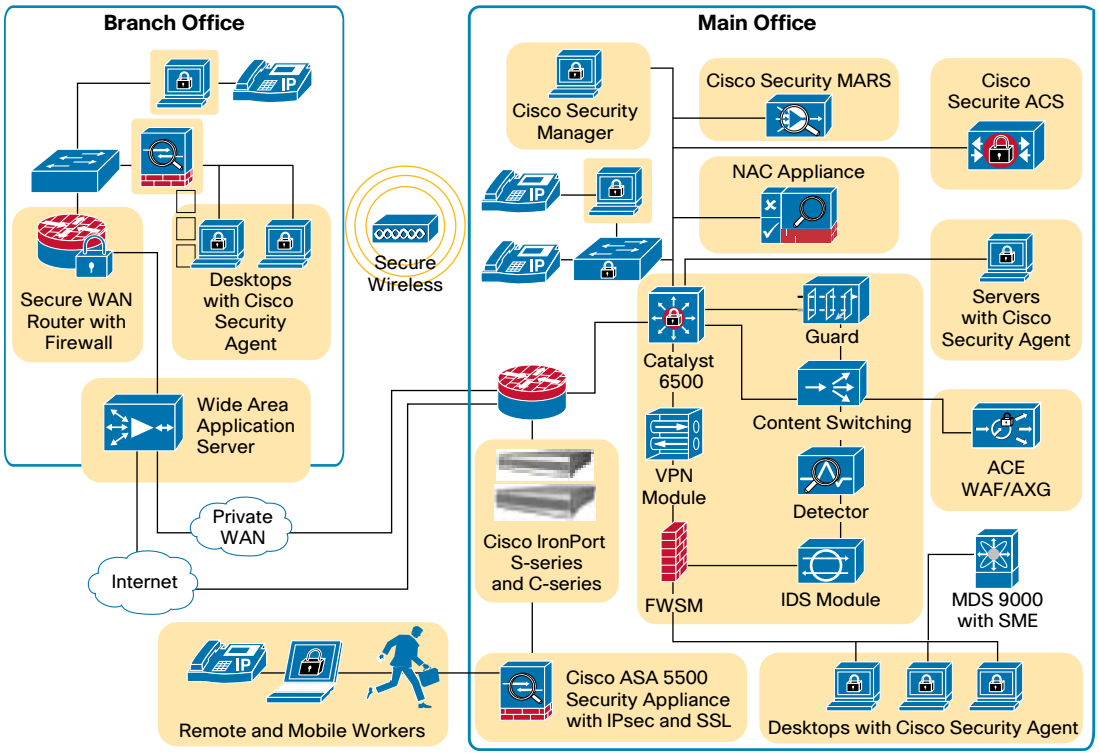
Putting It All Together

HOME

The Cisco® Self-Defending Network provides the most comprehensive, end-to-end approach to network security in the industry. Our world-class solutions not only provide best-of-breed capabilities and features, but also provide a level of security not available anywhere else, through:

1. Integration: Critical security functions have been woven into Cisco's entire line of appliances and network devices, as well as into all of our critical business applications and services, such as unified communications and data center.
2. Collaboration: An additional layer of security is achieved through unprecedented collaboration between security and network devices, and between different security devices and solutions.
3. Adaptability: The ability to identify a security event anywhere on the network, and share that information across the network, allows Cisco solutions to dynamically adapt the network's overall security profile to real-time threats and events.

This integrated, collaborative, and adaptive approach to security provides comprehensive, in-depth defense and maximum risk reduction, while lowering total cost of ownership, making it the ideal choice for securing your networked environment.



Contents

Why Security Matters More Than Ever

Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances

Firewall

Intrusion Prevention Systems

Cisco Router Security

End-Point Security
- Cisco Security Agent
- Cisco Network Admission Control

Email, Web, and Content Security
- Cisco Web Security Gateway Appliances
- Cisco IronPort Email Security Appliances
- Cisco ACE Web Application Firewall
- Content Security on the Cisco ASA 5500 Series

Management
- Cisco Security Monitoring, Analysis, and Response System
- Cisco Security Manager
- Cisco Secure Access Control System
- Cisco Enterprise Policy Manager

Switch Security
- Cisco Catalyst 6500 Series Security Services Modules
- Cisco TrustSec

Solutions
- Compliance
- Cisco Virtual Office

Virtual Private Networks
- Site-to-Site VPNs
- Remote-Access VPNs

Putting It All Together

EXIT