

## Cisco Integrated Firewall Solutions

Cisco ASA 5500 Series Adaptive Security Appliance, Cisco PIX Security Appliance, Cisco IOS Firewall, and the Firewall Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers

Networks are more critical to business success than ever before. They support key applications and processes and provide a common infrastructure for converged data, voice, and video services. Cisco Systems® understands the security challenges that organizations face today, and empowers its customers to safely engage in business by providing them with best in-class security solutions. Instead of only providing point products that set a base level of security, Cisco® philosophy is to embed security throughout the network and integrate security services in all of its products—resulting in greater security, and making security a transparent, scalable, and manageable aspect of the business infrastructure.

Cisco ASA 5500 Series adaptive security appliances, Cisco PIX® security appliances, the Cisco IOS® Advanced Security Feature Set, and the security services modules for Cisco Catalyst® 6500 Series switches and Cisco 7600 Series routers are integrated security solutions that best represent the Cisco security philosophy. Each of these products integrates comprehensive firewall, intrusion protection, and VPN technologies in a cost-effective, single-box format. Customers implementing these integrated solutions benefit from enhanced security, lower cost of ownership, and lower operational costs—all resulting from the increased intelligence sharing of integrated security services in a single platform.

### Integrated Firewall Solutions to Meet Every Need

The Cisco ASA 5500 Series, Cisco PIX security appliances, Cisco IOS Firewall, the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches, and Cisco 7600 Series routers are Cisco flexible integrated firewall solutions. Based on modular, scalable platforms, each offering is designed with a particular feature set to better secure different network environments. These solutions can be independently deployed to secure specific areas of the network infrastructure, or can be combined for a layered, defense-in-depth approach following the design best practices described in the Cisco SAFE Blueprint. Rounding out the integrated firewall solutions, Cisco provides a comprehensive security management product portfolio, ranging from Cisco Security Appliance and Cisco IOS Software security features and embedded device managers, to standalone management applications, helping to ensure that customers can effectively manage their Cisco security infrastructure investments.

### Cisco ASA 5500 Series

Cisco ASA 5500 Series adaptive security appliances are purpose-built solutions that bring together market-proven, best-of-breed security and VPN services with an innovative, adaptive architecture. The result is a powerful multifunction network security appliance better able to protect small and medium business (SMB) and enterprise networks and, at the same time, reduce the overall deployment and operations costs associated with this new level of security.

The Cisco ASA 5500 Series leverages technology developed for the Cisco PIX 500 Series Security Appliance, the Cisco IPS 4200 Series Intrusion Prevention System, and the Cisco VPN 3000 Series Concentrator. These technologies converge on the Cisco ASA 5500 Series to deliver a platform that stops the broadest range of threats. The Cisco ASA 5500 Series delivers application security, anti-X defense, network containment and control, and “clean” VPN connectivity across product portfolio (see Figure 1). This breadth of security enables protection of any network segment, including the most common threat conduits such as remote sites, LAN-attached internal users, and remote access VPNs.

**Figure 1.** Cisco ASA 5500 Series Appliance Portfolio

ASA 5510	ASA 5520	ASA 5540	ASA 5550
Medium Branch	Enterprise	Enterprise Edge	Enterprise Edge/HQ
			

**Note:** Figure 1 provides general guidelines. Network environments should be scaled based upon requirements.

The Cisco ASA 5500 Series provides strong application security through intelligent, application-aware inspection engines that examine network flows at Layers 4-7. The result is a more secure network including Web, voice, and 3G-mobile wireless services. To defend networks from application-layer attacks and to give businesses more control over the applications and protocols used in their environments, these inspection engines incorporate extensive application and protocol knowledge and employ security enforcement technologies that include protocol anomaly detection, and application and protocol state tracking. Also included are attack detection and mitigation techniques such as application/protocol command filtering, content verification, and URL deobfuscation. These inspection engines also deliver control over instant messaging, peer-to-peer file sharing, and tunneling applications, enabling businesses to enforce usage policies and free up network bandwidth for critical business applications.

While increasing network security, the Cisco ASA 5500 Series also decreases deployment and operational costs. Its broad VPN and security services profile makes it a single device for many uses, enabling platform standardization. It can be deployed as a converged threat-prevention device at the central site by leveraging its access control, application inspection, and worm, virus, and other malware mitigation technologies. It can also be used as a dedicated remote access device utilizing its VPN capabilities. Alternatively, it serves equally well in the network interior for interdepartmental access control and to guard against worms, viruses, and other malicious code internal users may unwittingly bring into the network. In small business and branch office environments, the Cisco ASA 5500 Series serves as an “all-in-one” device offering comprehensive threat prevention and VPN services while suiting the budgets and operational models of such deployments. This adaptive “single device, many uses” approach reduces the number of platforms that must be deployed and managed while offering a common operating and management environment across all those deployments. This approach simplifies configuration, monitoring, troubleshooting, and security staff training. To further minimize operations costs, the Cisco ASA 5500 Series is also highly network aware, enabling it to insert gracefully into the network without disrupting legitimate traffic and applications. (See Table 1.)

**Table 1.** Cisco ASA 5500 Series Firewall Performance




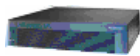
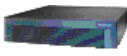
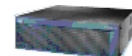
Firewall Performance
Cisco ASA 5510: 300 Mbps
Cisco ASA 5520: 450 Mbps
Cisco ASA 5540: 650 Mbps
Cisco ASA 5550: 1.2 Gbps

## Cisco PIX Security Appliances

The market-leading Cisco PIX Security Appliance Series delivers robust user and application policy enforcement, multivector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. These purpose-built appliances provide a wealth of integrated security and networking services, including advanced application-aware firewall services, market-leading voice over IP (VoIP) and multimedia security, robust site-to-site and remote-access IP Security (IPSec) VPN connectivity, award-winning resiliency, intelligent networking services, and flexible management solutions. The Cisco PIX Security Appliance family (Figure 2) ranges from compact “plug-and-play” desktop appliances for small and home offices to modular gigabit appliances with superior investment protection for enterprise and service-provider environments, Cisco PIX Security Appliances provide robust security, performance, and reliability for network environments of all sizes.

Cisco PIX security appliances integrate a broad range of advanced firewall services to protect businesses from the constant barrage of threats on the Internet and in business network environments. (See Figure 2.) As a secure foundation, Cisco PIX security appliances provide rich stateful inspection firewall services, tracking the state of all network communications and preventing unauthorized network access. Building upon those services, Cisco PIX security appliances deliver strong application layer security through intelligent, application-aware inspection engines that examine network flows at Layers 4-7. To defend networks from application-layer attacks and to give businesses more control over the applications and protocols used in their environments, these inspection engines incorporate extensive application and protocol knowledge and employ security enforcement technologies that include protocol anomaly detection, application and protocol state tracking, Network Address Translation (NAT) services, and attack detection and mitigation techniques such as application/protocol command filtering, content verification, and URL deobfuscation. These inspection engines also give businesses control over instant messaging, peer-to-peer file sharing, and tunneling applications, enabling businesses to enforce usage policies and free up network bandwidth for legitimate business applications.

**Figure 2.** Cisco PIX Security Appliance Portfolio

Cisco PIX 501	Cisco PIX 506E	Cisco PIX 515E	Cisco PIX 525	Cisco PIX 525	Cisco PIX 535
Teleworker/SO HO (1–20 users)	Small Branch (20–99 users)	Medium Branch (100–999 users)	Enterprise Branch (100–999 users)	Enterprise Edge	Enterprise HQ Data Center
					

**Note:** Figure 2 provides general guidelines. Network environments should be scaled on applications requirements, not solely on the size of the network.

Built upon a hardened, purpose-built operating system that delivers rich security services, Cisco PIX security appliances provide the highest levels of security and have earned many industry evaluations and certifications, including Common Criteria Evaluation Assurance Level (EAL) 4 status, as well as ICSA Labs Firewall and IP Security (IPSec) certification. Cisco PIX Security Appliances provide market-leading protection for a wide range of VoIP other multimedia standards including H.323 Version 4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), Media Gateway Control Protocol (MGCP), and others, helping businesses secure deployments of a wide range of current and next-generation VoIP and multimedia applications.

Cisco PIX security appliances deliver a wealth of configuration, monitoring, and troubleshooting options, giving businesses the flexibility to use the methods that best meet their needs. Management solutions range from centralized, policy-based management tools to integrated, Web-based management, to support for remote-monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog. The integrated Cisco Adaptive Security Device Manager (ASDM) provides a world-class Web-based management interface that greatly simplifies the deployment, ongoing configuration, and monitoring of a single Cisco PIX Security Appliance—without requiring any software (other than a standard Web browser and Java plug-in) to be installed on an administrator's computer. Administrators can also remotely configure, monitor, and troubleshoot Cisco PIX security appliances using a command-line interface (CLI). Secure CLI access is available using several methods, including Secure Shell (SSHv2) Protocol, Telnet over IPSec, and out-of-band through a console port. Cisco PIX security appliances also include robust auto-update capabilities, a set of revolutionary secure remote-management services that ensure firewall configurations and software images are kept up to date. In addition, Cisco PIX security appliances are supported by several configuration and monitoring tools available from Cisco AVVID (Architecture for Voice, Video and Integrated Data) partners.

Table 2 summarizes the firewall performance of each Cisco PIX Security Appliance model.

**Table 2.** Cisco PIX Security Appliance Firewall Performance

Firewall Performance
Cisco PIX 501: 60 Mbps
Cisco PIX 506E: 100 Mbps
Cisco PIX 515E: 190 Mbps
Cisco PIX 525: 330 Mbps
Cisco PIX 535: 1.7 Gbps









## Cisco IOS Firewall

The Cisco IOS Firewall is a stateful-inspection firewall option available for Cisco routers. Built from market-leading PIX Firewall technologies, Cisco IOS Firewall is supported on all the integrated services routers with the Cisco IOS Software Advanced Security or higher feature sets. Cisco IOS Firewall is an ideal single-box security and routing solution for protecting the WAN entry point into the network. The primary features of Cisco IOS Firewall include stateful firewall with denial of service (DoS) protection, enhanced application, traffic, and user awareness to identify, inspect, and control applications, advanced protocol inspection for voice, video, and other applications, per-user, interface, or subinterface security policies, tightly integrated identity services to provide per-user authentication and authorization, and ease of management. Fine-grained role-based

access enables secure, logical separation of router administration between Network Operations and Security Operations staff.

The Cisco IOS Firewall not only helps enable a single point of protection at the perimeter of a network, it also makes security policy enforcement an inherent component of the network itself. The Cisco IOS Firewall runs on numerous Cisco IOS routers and represents the best option for customers of small and medium-sized offices looking to leverage their network infrastructures for security, while continuing to take advantage of Cisco IOS Software capabilities, including quality of service (QoS), multiprotocol, multicast, and advanced routing support. (See Figure 3.)

**Figure 3.** Cisco IOS Firewall Portfolio

Cisco 871	Cisco 1841	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851	Cisco 3825	Cisco 3845
SOHO ECT	Small Branch	Medium Branch	Medium Branch	Medium Branch	Medium Branch	Enterprise Branch	Enterprise Branch
							

**Note:** Figure 3 provides general guidelines. Network environments should be scaled on the applications requirements, not solely on the size of the network.

The integrated Cisco IOS Firewall uses a sophisticated firewall engine capable of dynamically controlling traffic flows based on application-level intelligence, providing enhanced security for complex applications. The Cisco IOS Firewall also includes advanced application inspection and control for Hypertext Transport Protocol (HTTP) and e-mail. The Cisco IOS Firewall HTTP Inspection Engine enforces protocol conformance and prevents malicious or unauthorized behavior such as port 80 tunneling, malformed packets, and Trojans from passing through. The HTTP Inspection Engine provides Cisco IOS Firewall the intelligence to not only block non-HTTP traffic, but to help ensure traffic that is assumed to be HTTP is legitimate Web browsing and not Instant Messaging or other traffic trying to gain access through the firewall. The net result is that network administrators have more granular control of applications passing through the firewall.

Cisco integrated services routers also include an Intrusion Prevention System (IPS) that takes advantage of technology from the Cisco IDS Family. Cisco IOS IPS is an in-line, deep-packet, inspection-based solution that helps Cisco routers effectively mitigate network attacks. Because Cisco IOS Software IPS is in line, it can drop traffic, enabling the router to respond immediately to security threats and protect the network.

Cisco IOS IPSec has earned industry evaluations and certifications such as Common Criteria EAL 4 and ICSA Labs IPSec certification. Additional Cisco IOS Firewall capabilities include, voice traversal support, IPv6 support; transparent firewall; URL filtering; support for individual firewall contexts for VRF environments; Cisco Network Admission Control (NAC) support; failover support; Network Address Translation (NAT); time-based access lists; Java Applet blocking; peer router authentication; real-time alerts; audit trail; and event logging. Additionally, the Cisco IOS Firewall is ICSA Firewall certified.

The Cisco IOS Firewall can be managed using a convenient CLI through several methods, including Telnet, SSH, or out-of-band via a console port. Alternatively, the Cisco IOS Firewall can be configured and monitored using the Cisco Security Device Manager (SDM), an intuitive and secure Web-based device management tool embedded within Cisco IOS firewalls. Cisco SDM simplifies device and security configuration through smart wizards to enable customers to quickly

and easily deploy, configure, and monitor a Cisco IOS Firewall without requiring extensive knowledge of the Cisco IOS CLI. In addition, beginning with with Cisco IOS Software Release 12.3, Cisco IOS Firewall incorporates Cisco AutoSecure, a feature that eliminates the complexity of securing a router by automating the configuration of security features and the removal of insecure features enabled by default. This feature simplifies the security process, enabling a rapid implementation of security policies and procedures to ensure secure networking services. Cisco IOS Firewall can also be configured and monitored using tools available from Cisco AVVID partners.

Table 3 shows the firewall performance of different Cisco IOS router platforms running Cisco IOS Firewall. The performance numbers reflect the results of testing with both NAT and logging enabled.

**Table 3.** Cisco IOS Firewall Performance

Firewall Performance
Cisco 850: 10 Mbps
Cisco 870: 70 Mbps
Cisco 1841: 125 Mbps
Cisco 2801: 127 Mbps
Cisco 2811: 130 Mbps
Cisco 2851: 455 Mbps
Cisco 3825: 530 Mbps
Cisco 3845: 855 Mbps
Cisco 3845: 1.1 Gbps

### Cisco FWSM for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers

The Cisco FWSM is a high-speed, integrated firewall module for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers. The module provides the fastest firewall data rates in the industry—5 Gbps throughput, 100,000 connections per second (cps), and 1 million concurrent connections. Up to four Cisco FWSMs can be installed in the same chassis, providing an unmatched 20 Gbps of firewalling capacity per chassis. The FWSM can also be combined with other Cisco security service modules such as the Intrusion Detection Service Module (IDSM-2), IPSec VPN Service Module (VPNSM), and the Network Analysis Module (NAM-1 and NAM-2). This modular approach allows customers to leverage their existing switching and routing infrastructures at a low cost, while obtaining the highest performance available in the industry. The FWSM is an optimal solution for enterprise and service provider data centers, and enterprise campus distribution points.

Installed inside a Cisco Catalyst 6500 Series Switch or Cisco 7600 Series Internet Router, the FWSM allows any port on the device to operate as a firewall port and integrates stateful firewall security inside the network infrastructure. This becomes especially important where rack space is at a premium. The Cisco Catalyst 6500 emerges as the IP services switch of choice for customers requiring intelligent services such as firewall services, intrusion detection, and VPN, along with multilayer LAN, WAN, and MAN switching capabilities. (See Figure 4.)

**Figure 4.** Cisco FWSM for Catalyst 6500 Series Switches and Cisco 7600 Series Routers

The Cisco FWSM is based on Cisco PIX technology and uses the same time-tested Cisco PIX operating system—a secure, real-time operating system. The FWSM offers a unique combination of performance and security on the same platform, using proven Cisco PIX technology for inspecting packets.

The Cisco FWSM is supported by the CiscoView Device Manager (CVDM) for Cisco Catalyst 6500 Series switches to perform initial setup and to provide graphical VLAN virtualization across all services. The embedded manager, the Cisco PIX Device Manager (PDM) for advanced configuration, monitoring, and troubleshooting, can also be launched from CVDM. Additionally, the FWSM is supported by Cisco AVVID partners for configuration, monitoring, and reporting.

### When to Deploy Each Cisco Integrated Firewall Solution

Cisco ASA 5500 Series, Cisco PIX security appliances, the Cisco IOS Firewall, and the Cisco FWSM all incorporate leading-edge firewall technologies and have many benefits and features in common; however, each solution has been specifically engineered for specific environments. The following tables show the similarities and differences of these solutions, and provide the general guidelines to help network designers decide when to deploy each solution and how to take maximum advantage of their individual capabilities. (See Tables 4-8.)

**Table 4.** Features and Benefits Common to the Cisco ASA 5500 Series, Cisco PIX Security Appliance, Cisco IOS Firewall, and the Cisco FWSM

Feature	Benefit
<b>Stateful Inspection Firewall</b>	Provides robust network and application security by enforcing administrator-defined access control policies while performing deep packet inspection and tracking the state of all network communications.
<b>Application/Protocol Inspection and Control</b>	Delivers enhanced application and protocol security by using specialized inspection engines capable of examining data streams at Layers 4-7.
<b>Dynamic, Per-User Authentication and Authorization</b>	Provides flexible user authentication and authorization via the high performance cut-through proxy mechanism and integration with Cisco Secure Access Control Sever (ACS) using Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) protocols, which allows for integration into numerous user databases, including Microsoft Active Directory, Microsoft Windows NT domains, LDAP directories, and one-time password systems.
<b>Dynamic and Static NAT and Port Address Translation (PAT)</b>	Provides extensive NAT application and protocol support and protects internal network addresses from the outside, providing an additional level of security.
<b>Content Filtering</b>	Improves employee productivity through integration with leading third-party URL filtering solutions; supports URL filtering and blocks malicious Java applets.
<b>Remote Management</b>	Offers a wealth of remote-management methods for configuration, monitoring, and troubleshooting. Management solutions range from highly scalable, centralized management tools to integrated, Web-based management, to support for remote-monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog.

Feature	Benefit
<b>Administrative Access Control Based on Authentication, Authorization, and Accounting (AAA)</b>	Provides granular control for administrative access based on the AAA services provided by the TACACS+ and RADIUS protocols. This allows administrators to enforce access policies to the level of what services and commands are allowed to each admin user or group.
<b>Multiple DMZ Support</b>	Supports additional physical or virtual network interfaces that can provide protected access to servers (such as Web, e-mail, FTP, or DNS) on a shared network (DMZ).
<b>Extensive Multimedia Support, Including Streaming Video, Streaming Audio, and Voice Applications</b>	Provides rich stateful inspection firewalling services for wide range of VoIP standards and other multimedia standards, allowing businesses to securely take advantage of the many benefits that converged data, voice, and video networks provide, such as improved productivity and competitive advantage.
<b>DoS Protection</b>	Provides several mechanisms to block and mitigate DoS attacks, such as TCP Intercept, TCP SYN cookies, DNS Guard, Flood Defender, Flood Guard, Mail Guard, and Unicast Reverse Path Forwarding (uRPF).
<b>Secure Dynamic Routing</b>	Supports Message Digest Algorithm 5 (MD5)-based and plain-text routing authentication for Routing Information Protocol (RIP) and Open Shortest Path First (OSPF), preventing route spoofing and various routing-based DoS attacks.
<b>Firewall Virtualization</b>	Enables the device to be partitioned into multiple virtual firewalls, or security contexts. Organizations can manage each of these virtual firewalls separately and can segregate business units or other functional areas on the same physical infrastructure. Similarly, service providers can leverage firewall virtualization to support and segregate multiple customers on a single physical device.

**Table 5.** When to Choose Cisco ASA 5500 Adaptive Security Appliances

Customer Requirement	Cisco ASA 5500 Security Appliance Benefit
<b>Purpose-Built, Best-of-Breed, “Converged” Security Appliance</b>	Cisco ASA Series devices provide state-of-the-art integrated network security services, including stateful inspection firewalling, IPS, VPN, worm and malware mitigation, network anti-virus, VPN clustering, and a modular security services slot. Note that Cisco ASA 5500 Series devices are fully compatible with Cisco PIX appliances, and deployments can leverage both to meet customer requirements.
<b>Single Security Appliance with Multiple Uses For Headends and Branch Offices</b>	Cisco ASA Series can be deployed as converged threat prevention devices at central sites by leveraging its access control, application inspection, and worm, virus, and malware mitigation technologies. They can be deployed as remote access devices utilizing their IPSec and SSL VPN capabilities. In the network interior, they can be used for inter-departmental access control and to guard against worms, viruses, and other malicious code internal users may unwittingly bring into the network. In each of these instances, the Cisco ASA device represents the most feature-rich Cisco solution.
<b>Converged Appliance with Reduced Operating Costs</b>	The “single device, many uses” approach reduces the number of platforms that must be deployed and managed, while offering a common operating and management environment across all those deployments. This approach simplifies configuration, monitoring, troubleshooting, and security staff training.
<b>High Availability</b>	When configured as failover pairs, Cisco ASA 5500 security appliances provide stateful failover, with synchronized connection-state and device-configuration data. This ensures network sessions are automatically transitioned between appliances with absolute transparency to users.

**Table 6.** When to Choose Cisco PIX Security Appliances

Customer Requirement	Cisco PIX Security Appliance Benefit
<b>Purpose-Built, Best-of-Breed, All-In-One Security Appliance</b>	Cisco PIX security appliances provide state-of-the-art, integrated network security services, including stateful inspection firewalling, protocol and application inspection, VPNs, inline intrusion protection, and rich multimedia and voice security. Note that Cisco PIX security appliances are fully compatible with Cisco ASA 5500 Series devices, and deployments can leverage both to meet customer requirements.
<b>Dedicated Device for Enterprise Headends and Data Centers</b>	Cisco PIX security appliances are security-specialized and run a hardened, embedded operating system, eliminating the common security holes of general purpose operating systems, and providing an unmatched system of overall security.

Customer Requirement	Cisco PIX Security Appliance Benefit
<b>Separated Security Infrastructure</b>	Cisco PIX security appliances can be implemented as dedicated security systems that provide advanced security features that allow an effective segregation of the security infrastructure from the rest of the network.
<b>High Availability</b>	Like the ASA 5500 Series appliances, when configured as failover pairs, Cisco PIX security appliances provide stateful failover with synchronized connection-state and device-configuration data. This ensures network sessions are automatically transitioned between appliances, with absolute transparency to users.
<b>Appliances for Small Office/Home Office</b>	The Cisco PIX 501 Security Appliance provides a wide range of rich, integrated security services, advanced networking services, and powerful remote management capabilities in a compact, all-in-one security solution. It delivers enterprise-class security for small office and teleworker environments, in a reliable, easy-to-deploy, purpose-built appliance.

**Table 7.** When to Choose Cisco IOS Firewall

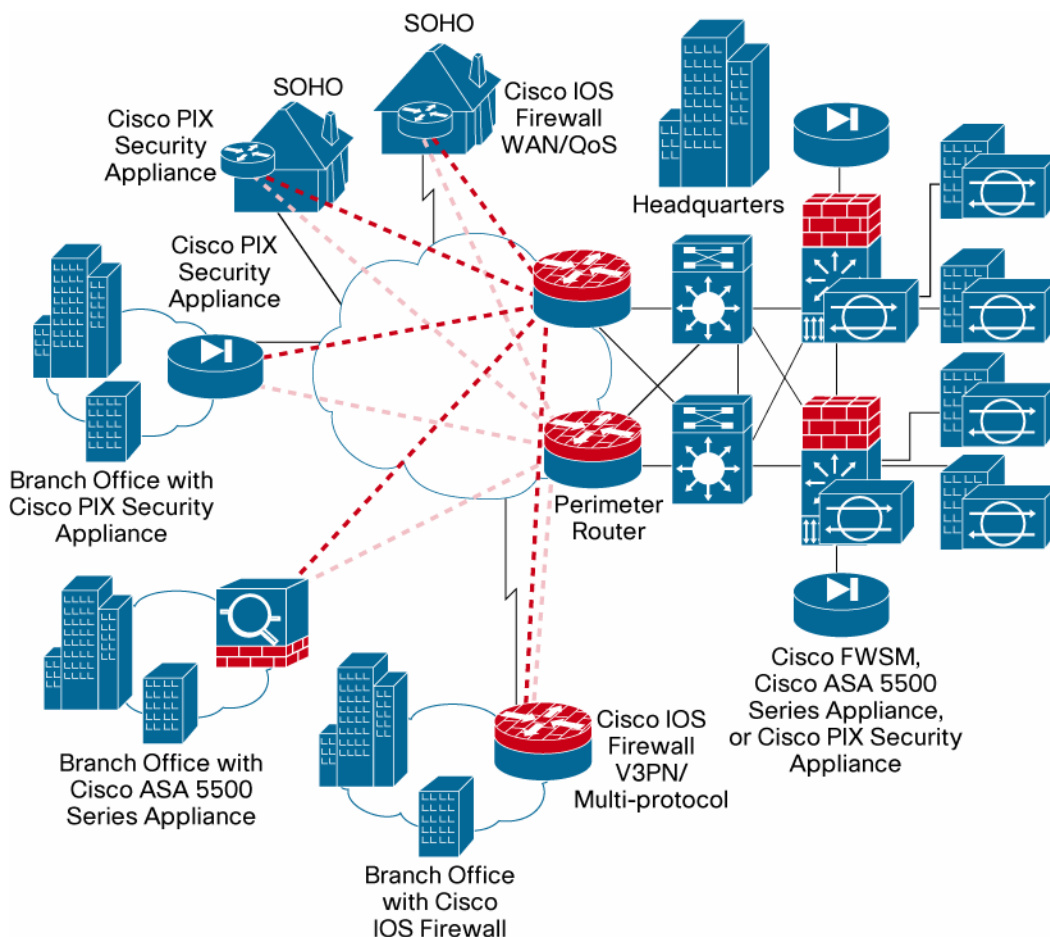
Customer Requirement	Cisco IOS Firewall Benefit
<b>One-Box Solution Combining Powerful Security, QoS, Multiprotocol Routing, Integrated WAN Interfaces, and Voice Application Support</b>	The Cisco IOS Advanced Security Feature Set provides a comprehensive, integrated security solution, including stateful packet filtering, intrusion detection and protection, per-user authentication and authorization, VPN capability, extensive QoS mechanisms, multiprotocol routing, voice application support, and integrated WAN interface support in one box.
<b>Leverage Network Infrastructure for Security</b>	The Cisco IOS Firewall can be loaded on existing Cisco IOS routers, providing greater investment protection in the network infrastructure. Reusing the same hardware chassis and components not only reduces the cost of ownership, but also the costs of operation—the same management infrastructure can be used and no additional staff training is required.
<b>Extensive VPN Support Integrated with Firewalling In A Single Device</b>	Deploying Cisco IOS Firewall with Cisco IOS encryption and QoS VPN features enables secure, low-cost transmissions over public networks. Cisco IOS Firewall provides the most extensive VPN support, including but not limited to Dynamic Multipoint VPN (DMVPN), IPsec stateful failover, Easy VPN Remote, Easy VPN Server, site-to-site VPNs, Advanced Encryption Standard (AES), VPN acceleration cards, Voice and Video-Enabled VPN (V3PN), and VPN QoS.

**Table 8.** When to Choose Cisco FWSM

Customer Requirement	Cisco FWSM Benefit
<b>Service Provider and Large Enterprise Headends and Data Centers</b>	The performance, scalability and virtualization capabilities of the Cisco FWSM make it ideally suited for service providers and large enterprise headends and data centers. The Cisco FWSM provides the highest firewall performance in the industry—5 Gbps throughput, 100,000 connections per second (cps), and 1 million concurrent connections. Up to four FWSMs can be deployed in the same chassis for a total of 20 Gbps of throughput. A single FWSM can support up to 1000 virtual interfaces (256 per context), and a single chassis can scale up to a maximum of 4000 VLANs. A single FWSM can be partitioned into up to 100 virtual firewalls (security contexts). Using the FWSM Resource Manager, organizations can limit the resources allocated to any security context at any time, which helps to ensure that one security context does not interfere with another.
<b>Leverage Network and Switching Infrastructure at the Headend or Data Center</b>	The Cisco FWSM can be deployed in existing Cisco Catalyst 6500 Series switches or Cisco 7600 Series routers, providing greater investment protection and integration with high-speed switching and routing. In addition, the FWSM can be deployed both in transparent Layer 2 bridging mode or in Layer 3 routing mode. A transparent Layer 2 firewall simplifies network integration and allows traffic to be firewalled within the same subnet without any routing involved.
<b>High Availability</b>	The Cisco FWSM can be deployed in pairs to provide intra- or inter-chassis stateful failover services that ensure resilient network protection for the most critical environments. Modules configured in failover mode continuously synchronize their connection state and device configuration data, and in the event of failure, modules failover with absolute transparency to users.

Figure 5 illustrates how Cisco integrated firewall solutions can be deployed together to secure an enterprise network.

**Figure 5.** How Cisco Integrated Security Solutions Secure Your Enterprise Network



### Cisco Security Management Solutions

In addition to the embedded device managers on the Cisco Firewall Solutions, Cisco provides integrated security management applications for customers who want to manage more than the 1-5 devices that the embedded managers are designed for.

For customers looking for comprehensive security management, policy administration, monitoring, and analysis for Cisco Firewall Solutions, Cisco provides the CiscoWorks VPN/Security Management Solution (VMS). CiscoWorks VMS is an integral part of the Cisco SAFE Blueprint for enterprise network security, and protects the productivity of organizations by combining Web-based tools for configuring, monitoring, and troubleshooting VPNs, firewalls, and network- and host-based intrusion detection systems (IDSs). CiscoWorks VMS delivers VPN configuration management, firewall management, surveillance, device inventory, and software version management features from a single management console.

For centralized security information management, Cisco offers the Cisco Security Monitoring, Analysis and Response System (MARS). Cisco Security MARS is a family of high-performance, scalable threat-mitigation appliances that fortify network devices and security countermeasures. By combining network topology intelligence, context correlation, analysis and auto-mitigation

capabilities, Cisco Security MARS is able to identify, manage, and eliminate network attacks and maintain compliance.

For large-scale enterprise customers and service providers, Cisco also offers the CiscoWorks Security Information Management Solution (SIMS). With CiscoWorks SIMS, customers can manage a growing multivendor security infrastructure without increasing the size of existing security staff. CiscoWorks SIMS lets customers normalize, aggregate, correlate, and visualize the thousands of security alerts received every day from security devices and applications. CiscoWorks SIMS is available for ordering as a software-only option that provides the flexibility to implement a multitier server architecture that is suitable for larger deployments; and as an appliance option, which consists of the CiscoWorks SIMS pre-installed on the Cisco 1160 hardware solution platform.

For customers looking to offer firewall managed services built on Cisco firewall solutions, Cisco offers the Cisco IP Solution Center (ISC). Cisco ISC implements a business-centric, policy-level management model that allows customers to define high-level security policies, while the application of those policies to specific network devices is offloaded to the Cisco ISC software. The Cisco ISC Security Management Module provides full support for the provisioning and management of LAN-to-LAN VPN, remote-access VPN, EZ VPN, DMVPN, firewall, NAT, and QoS technologies for numerous Cisco security devices (Cisco IOS Firewall, Cisco PIX Security Appliance, and Cisco VPN 3000 Series Concentrator, for example).

### Ordering Information

To place an order, visit the [Cisco Ordering Home Page](#).

### Additional Information

For more information, please visit the following links:

- Cisco ASA 5500 Series Security Appliance: <http://www.cisco.com/go/asa>
- Cisco PIX Security Appliance Series: <http://www.cisco.com/go/pix>
- Cisco IOS Firewall: <http://www.cisco.com/go/firewall>
- Router Security from Cisco: <http://www.cisco.com/go/routersecurity>
- Cisco Firewall Services Module:  
<http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html>
- Cisco PIX Device Manager:  
<http://www.cisco.com/en/US/products/sw/netmgtsw/ps2032/index.html>
- Cisco Security Device Manager:  
<http://www.cisco.com/en/US/products/sw/secursw/ps5318/index.html>
- CiscoWorks VMS: <http://www.cisco.com/en/US/products/sw/cscowork/ps2330/index.html>
- Cisco ISC: <http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/index.html>
- CiscoWorks SIMS: <http://www.cisco.com/en/US/products/sw/cscowork/ps5209/index.html>
- SAFE Blueprint from Cisco: <http://www.cisco.com/go/safe>

**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**

Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**

Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)