

Cisco Integrated Firewall Solutions

Cisco® ASA 5500 Series Adaptive Security Appliance, Cisco PIX® Security Appliance, Cisco IOS® Firewall in Cisco Integrated Services Routers and Cisco ASR 1000 Series Aggregation Services Routers, and the Firewall Services Module (FWSM) for Cisco Catalyst® 6500 Series Switches and Cisco 7600 Series Routers.

Networks are more critical to business success than ever before. They support critical applications and processes and provide a common infrastructure for converged data, voice, and video services. Cisco 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 providing only point products that set a base level of security, Cisco embeds security throughout the network and integrates security services in all of its products--heightening security and making it 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 in Cisco integrated services routers and Cisco ASR 1000 Series Aggregation Services Routers, and the FWSM 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 prevention, and VPN technologies in a cost-effective, single-box format. Customers who implement 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, and the 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. You can deploy these solutions independently to secure specific areas of your network infrastructure, or combine them for a layered, defense-in-depth approach following the design best practices described in the SAFE Blueprint from Cisco.

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 you can effectively manage your Cisco security infrastructure.

Cisco ASA 5500 Series

Cisco ASA 5500 Series Adaptive Security Appliances bring together market-proven, best-in-class security and VPN services with an innovative, adaptive architecture. The result is a powerful multifunction network security appliance that protects small and medium-sized businesses (SMBs), enterprises, and data center networks--while reducing the overall deployment and operations costs associated with this new level of security.

The Cisco ASA 5500 Series uses technology developed for the Cisco PIX 500 Series Security Appliance, the Cisco IPS 4200 Series Sensors, and the Cisco VPN 3000 Series Concentrators. These technologies converge in the Cisco ASA 5500 Series to deliver a platform that stops the broadest range of threats. The Cisco ASA 5500 Series delivers application security, content security, and “clean” VPN connectivity across its product portfolio (Figure 1). This breadth of security protects 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

| Cisco ASA 5505 | Cisco ASA 5510 | Cisco ASA 5520 | Cisco ASA 5540 | Cisco ASA 5550 | Cisco ASA 5580 |
|---|---|---|--|---|---|
| Small Office | Medium-Sized Branch Office | Enterprise | Enterprise Edge | Enterprise Edge or Headquarters | Data Center |
|  |  |  |  |  |  |

Note: Figure 1 provides general guidelines. You should scale your network based upon your 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 third-generation (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 and 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 your business to enforce usage policies and free 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. You can deploy it as a converged threat-prevention device at the central site by using its access control, application inspection, and worm, virus, and other malware mitigation technologies. You can also use it as a dedicated remote-access device employing its VPN capabilities. It serves equally well in the network interior for interdepartmental access control and as a guard against worms, viruses, and other malicious code that 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 you must deploy and manage 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, inserting gracefully into the network without disrupting legitimate traffic and applications.

Cisco ASA 5500 Series Firewall Performance

- Cisco ASA 5505: 150 Mbps
- Cisco ASA 5510: 300 Mbps
- Cisco ASA 5520: 450 Mbps
- Cisco ASA 5540: 650 Mbps
- Cisco ASA 5550: 1.2 Gbps
- Cisco ASA 5580-20: 6.5 Gbps
- Cisco ASA 5580-40: 14 Gbps

Cisco PIX Security Appliances

The market-leading Cisco PIX Family of security appliances delivers robust user and application policy enforcement, multivector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. These 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.

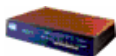


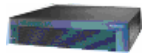
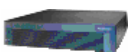
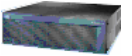
The Cisco PIX Family ranges from compact, ready-to-use desktop appliances for small and home offices to modular gigabit appliances with superior investment protection for enterprise and service provider environments. Cisco PIX security appliances provide robust security, performance, and reliability 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 (Figure 2). The appliances provide rich stateful inspection firewall services, tracking the state of all network communications and preventing unauthorized network access.

They also 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 your business more control over the applications and protocols used in your 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 and protocol command filtering, content verification, and URL deobfuscation.

These inspection engines also give your business control over instant messaging, peer-to-peer file sharing, and tunneling applications, enabling you to enforce usage policies and free 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 or SOHO (1–20 Users) | Small Branch Office (20–99 Users) | Medium-Sized Branch Office (100–999 Users) | Enterprise Branch Office (100–999 Users) | Enterprise Edge | Enterprise Headquarters Data Center |
|  |  |  |  |  |  |

Note: Figure 2 provides general guidelines. You should scale your network on applications requirements, not solely on the size of your network.

Built upon a hardened OS 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 for Firewall and IPsec certification. Cisco PIX security appliances provide market-leading protection for a wide range of VoIP and 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 your business the flexibility to use the methods that best meet your 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 Version 2 (SSHv2) Protocol, Telnet over IPsec, and out of band through a console port. Cisco PIX security appliances also include robust autoupdate capabilities, a set of revolutionary secure remote-management services that help ensure that 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 Technology Developer Partners.

The firewall performance of each Cisco PIX security appliance model follows:

Cisco PIX Security Appliance 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 1800, 2800, and 3800 Series Integrated Services Routers; Cisco 800 and 7200 Series Routers; Cisco ASR 1000 Series Aggregation Services Routers; and Cisco 7301 Routers. Cisco IOS Firewall is supported on all integrated services routers with Cisco IOS Software Advanced Security or higher feature sets. Zone-based Cisco IOS Firewall is also supported at multigigabit rates on the [Cisco ASR 1000 Series Aggregation Services Routers](#) for the WAN and Internet edge in enterprise networks and for broadband subscribers in service provider networks.

Cisco IOS Firewall is an ideal single-box security and routing solution for protecting the WAN entry point into the network. Its primary features 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, per-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.

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 Software-based routers (see Figure 3). It represents the best option for customers--regardless of office size--that want to use the network infrastructure for security, while continuing to take advantage of Cisco IOS Software capabilities, including quality of service (QoS), multiprotocol, multicast, and advanced routing support.

Figure 3. Cisco IOS Firewall Portfolio

| Cisco 871 | Cisco 1841 | Cisco 2801 | Cisco 2811 | Cisco 2821 | Cisco 2851 | Cisco 3825 | Cisco 3845 | Cisco ASR 1000 Series |
|---|---|---|---|---|--|---|---|---|
| SOHO Enterprise Class Teleworker (ECT) | Small Branch Office | Medium-Sized Branch Office | Medium-Sized Branch Office | Medium-Sized Branch Office | Medium-Sized Branch Office | Enterprise Branch Office | Enterprise Branch Office | Enterprise WAN Edge and High-Speed Branch Office, Service Provider Broadband |
|  |  |  |  |  |  |  |  |  |

Note: Figure 3 provides general guidelines. You should scale your network 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. It also includes advanced application inspection and control for HTTP and email messages. The Cisco IOS Firewall HTTP Inspection Engine enforces protocol conformance and prevents malicious or unauthorized behavior such as port 80 tunneling, malformed packets, and Trojan horses from passing through. The HTTP Inspection Engine gives 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 result is that network administrators have greater control of applications passing through the firewall.

Cisco integrated services routers also include an intrusion prevention system (IPS) that takes advantage of Cisco IPS technology. Cisco IOS IPS is an inline, deep-packet-inspection-based solution that helps Cisco routers effectively mitigate network attacks. Because Cisco IOS IPS is inline, it can drop traffic, enabling the router to respond immediately to security threats and protect the network.

Additional Cisco IOS Firewall capabilities include voice traversal support; IPv6 support; transparent firewall; URL filtering; support for individual firewall contexts for Virtual Route Forwarding (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 trails; and event logging. Cisco IOS Firewall is CC EAL4 certified, and Cisco IOS IPsec is FIPS 140-2 certified.

You can manage Cisco IOS Firewall through a convenient CLI using several methods, including Telnet, SSH, or out-of-band management through a console port. Alternatively, you can configure and monitor Cisco IOS Firewall using Cisco Configuration Professional (CCP), an intuitive and secure web-based device management tool embedded within Cisco IOS Firewalls. Cisco CP simplifies device and security configuration through smart wizards that 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 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. You also can configure and monitor Cisco IOS Firewall using tools available from Cisco Technology Developer Partners.

Cisco ASR 1000 Series: A Powerful New Paradigm for the WAN Edge

The new Cisco ASR 1000 Series Aggregation Services Router uses the Cisco QuantumFlow Processor--the industry's first massive parallel processor hardware and software architecture--to deliver high-performance integrated threat control services such as firewall, deep packet inspection, and logging services, concurrent with WAN and Internet edge routing.

Cisco ASR 1000 Series routers make a compelling case for integrating attack identification and prevention into the enterprise WAN and Internet edge router:

- Cisco IOS Firewall services scale up to 5, 10, and 20 Gbps. You can apply zone-based firewall policies on all Cisco ASR 1000 Series Router interfaces.
- Deep packet inspection with Network Based Application Recognition (NBAR) and Flexible Packet Matching (FPM) is processed at multigigabit rates, along with high-speed logging (40,000 sessions per second) using Cisco NetFlow v9.

Cisco IOS Firewall is supported on all Cisco ASR 1000 Series Aggregation Services Routers with the Cisco IOS XE ASR 1000 Series Route Processor 1 (RP1) and Route Processor 2 (RP2) Advanced IP Services software and Advanced Enterprise Services image options (including those without crypto).

Cisco ASR 1000 Series firewall delivers up to 20 Gbps performance in a carrier-class WAN. It is positioned between the Cisco 7200 Series and the Firewall Services Module for the Cisco 7600 Series and Cisco Catalyst 6500 Series.

For more information about the Cisco ASR 1000 Series, visit <http://www.cisco.com/go/asr1000>.

The following list specifies the firewall performance of different Cisco IOS router platforms running Cisco IOS Firewall. These performance numbers reflect the results of testing with stateful inspection applied to HTTP traffic containing 64-KB objects.

Cisco IOS Firewall Performance

- Cisco 870: 32 Mbps
- Cisco 1811: 93 Mbps
- Cisco 1841: 93 Mbps
- Cisco 1861: 90 Mbps
- Cisco 2801: 45 Mbps
- Cisco 2811: 94 Mbps
- Cisco 2821: 352 Mbps
- Cisco 2851: 452 Mbps
- Cisco 3825: 564 Mbps
- Cisco 3845: 729 Mbps
- Cisco ASR 1000 Series: 5, 10, or 20 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 industry-leading data rates: 5 Gbps throughput; 100,000 connections per second (cps); and 1 million concurrent connections.

You can install up to four Cisco FWSMs in the same chassis, for an unmatched 20 Gbps of firewalling capacity per chassis. You can also combine the Cisco FWSM with other Cisco security services modules such as the Intrusion Detection Services Module (IDSM-2), IPsec VPN Service Module (VPNSM), and the Network Analysis Module (NAM-1 and NAM-2). This modular approach allows you to take advantage of your existing switching and routing infrastructures while obtaining the highest performance available in the industry; no costly upgrades are needed. 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 Router, the Cisco FWSM (Figure 4) allows any port on the device to operate as a firewall port and integrates stateful firewall security inside the network infrastructure. This feature becomes especially important where rack space is at a premium. The Cisco Catalyst 6500 Series is the IP services switch of choice for customers requiring intelligent services such as firewall services, intrusion detection, and VPN services, along with multilayer LAN, WAN, and MAN switching capabilities.

Figure 4. Cisco FWSM for Cisco 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 Cisco 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 for Cisco Catalyst 6500 Series Switches to perform initial setup and to provide graphical VLAN virtualization across all services. You can also launch Cisco PIX Device Manager, the embedded manager for advanced configuration, monitoring, and troubleshooting, from CiscoView Device Manager. Additionally, the Cisco FWSM is supported by Cisco Technology Developer Partners for configuration, monitoring, and reporting.

When to Deploy Each Cisco Integrated Firewall Solution

Cisco ASA 5500 Series, Cisco PIX security appliances, 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 designed for specific environments. Tables 1–4 show the similarities and differences of these solutions, and provide general guidelines to help network designers decide when to deploy each solution and how to take maximum advantage of their individual capabilities.

Table 1. Features and Benefits Common to the Cisco ASA 5500 Series, Cisco PIX Security Appliance, Cisco IOS Firewall, and the Cisco FWSM

| Feature | Benefit |
|---|--|
| Stateful Inspection Firewall | 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. |
| Application and protocol inspection and control | Delivers enhanced application and protocol security by using specialized inspection engines capable of examining data streams at Layers 4–7. |
| Dynamic, per-user authentication and authorization | Provides flexible user authentication and authorization through the high-performance cut-through proxy mechanism and integration with Cisco Secure Access Control Sever (ACS) using RADIUS and TACACS+ protocols. It allows for integration into numerous user databases, including Microsoft Active Directory, Microsoft Windows NT domains, Lightweight Directory Access Protocol (LDAP) directories, and one-time password systems. |
| Dynamic and Static NAT and | Provides extensive NAT application and protocol support and protects internal network addresses from the |

| Feature | Benefit |
|---|--|
| Port Address Translation (PAT) | outside, providing an additional level of security. |
| Content filtering | Improves employee productivity through integration with leading third-party URL filtering solutions; it supports URL filtering and blocks malicious Java applets. |
| Remote management | 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 SNMP and syslog. |
| Administrative access control based on authentication, authorization, and accounting (AAA) | Provides granular control for administrative access based on the AAA services provided by the TACACS+ and RADIUS protocols, allowing administrators to enforce access policies to the level of what services and commands are allowed to each admin user or group. |
| Multiple DMZ support | Supports additional physical or virtual network interfaces that can provide protected access to servers (such as web, email messaging, FTP, or Domain Name System [DNS]) on a shared network (DMZ). |
| Extensive multimedia support, including streaming video, streaming audio, and voice applications | Provides rich stateful inspection firewall 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. |
| DoS attack protection | 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). |
| Secure dynamic routing | Supports Message Digest Algorithm 5 (MD5)-based and plaintext routing authentication for Routing Information Protocol (RIP) and Open Shortest Path First (OSPF), preventing route spoofing and various routing-based DoS attacks. |
| Firewall virtualization | Enables the device to be partitioned into multiple virtual firewalls or security contexts. Organizations can manage each virtual firewall separately and can segregate business units or other functional areas on the same physical infrastructure. Similarly, service providers can use firewall virtualization to support and segregate multiple customers on a single physical device. |

Table 2. When to Choose Cisco ASA 5500 Adaptive Security Appliances

| Customer Requirement | Cisco ASA 5500 Security Appliance Benefit |
|---|---|
| Purpose-built, best-in-class, “converged” security appliance | Cisco ASA 5500 Series devices provide state-of-the-art integrated network security services, including stateful inspection firewall, IPS, VPN, worm and malware mitigation, network antivirus, and VPN clustering services, along with a modular security services slot. Cisco ASA 5500 Series devices are fully compatible with Cisco PIX devices; you can use appliances from both families to meet customer requirements. |
| Single security appliance with multiple uses for headends and branch offices | You can deploy Cisco ASA 5500 Series appliances as converged threat-prevention devices at central sites by using their access control, application inspection, and worm, virus, and malware mitigation technologies. You can also deploy them as remote-access devices using their IPsec and SSL VPN capabilities. You can use them 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 each of these instances, the Cisco ASA device represents the most feature-rich Cisco solution. |
| Converged appliance with reduced operating costs | The “single device, many uses” approach reduces the number of platforms that you must deploy and manage, while offering a common operating and management environment across all those deployments. This approach simplifies configuration, monitoring, troubleshooting, and security staff training. |
| High availability | When configured as failover pairs, Cisco ASA 5500 Series appliances provide stateful failover, with synchronized connection-state and device-configuration data, helping ensure that network sessions are automatically transitioned between appliances with full transparency to users. |

Table 3. When to Choose Cisco PIX Security Appliances

| Customer Requirement | Cisco PIX Security Appliance Benefit |
|--|---|
| Purpose-built, best-in-class, all-in-one security appliance | Cisco PIX security appliances provide state-of-the-art, integrated network security services, including stateful inspection firewall, protocol and application inspection, VPNs, inline intrusion prevention, and rich multimedia and voice security services. Cisco PIX security appliances are fully compatible with Cisco ASA 5500 Series devices; deployments can use both to meet customer requirements. |
| Dedicated device for enterprise headends and data centers | 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 a superior system of overall security. |
| Separated security infrastructure | You can implement Cisco PIX security appliances as dedicated security systems that provide advanced security features that allow an effective segregation of the security infrastructure from the rest of the network. |
| High availability | Like the Cisco 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 helps ensure that network sessions are automatically transitioned between appliances, with full transparency to users. |
| Appliances for the small office and home office | 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 4. When to Choose Cisco IOS Firewall

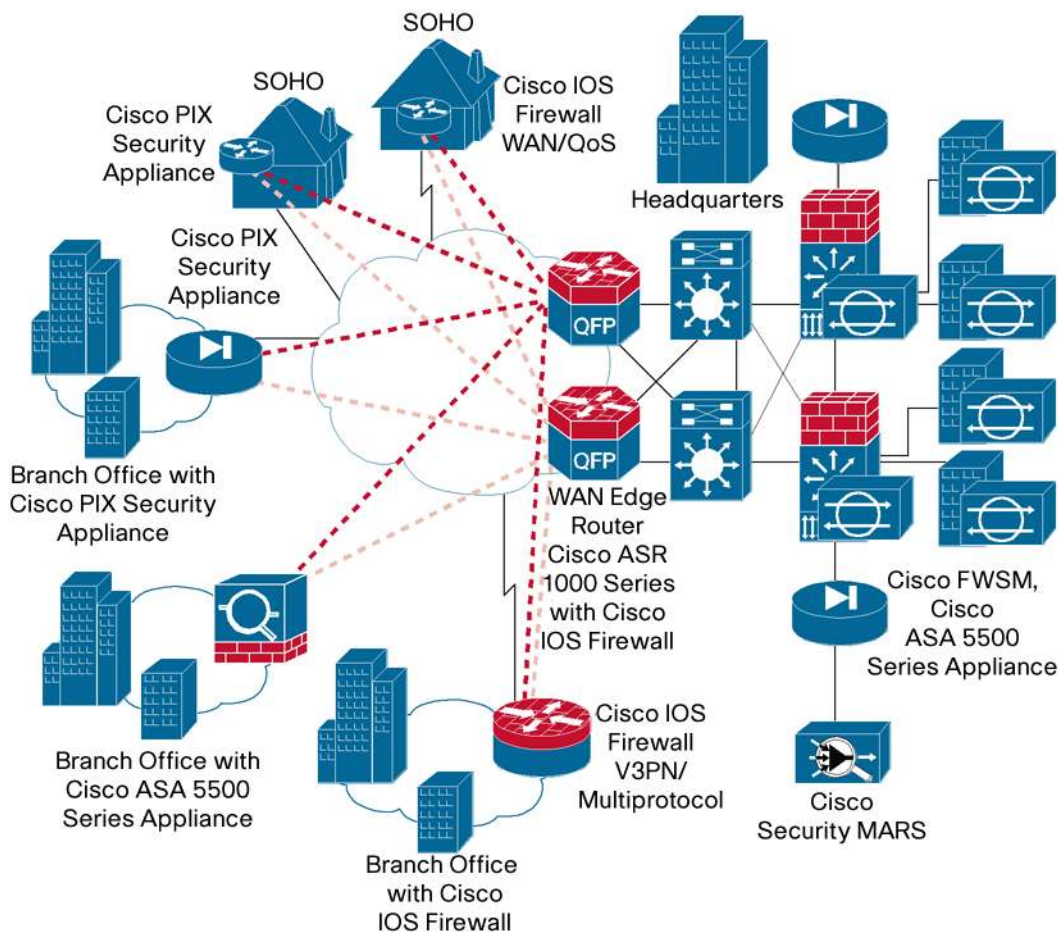
| Customer Requirement | Supported Platform | Cisco IOS Firewall Benefit |
|---|---|---|
| One-box solution combining powerful security, QoS, multiprotocol routing, integrated WAN interfaces, and voice application support | Cisco 800, 1800, 2800, and 3800 Integrated Services Routers, the Cisco 7200 Router, and Cisco ASR 1000 Series | The Cisco IOS Software Advanced Security Feature Set provides a comprehensive, integrated security solution, including stateful packet filtering, intrusion detection and prevention, per-user authentication and authorization, VPN capability, extensive QoS mechanisms, multiprotocol routing, voice application support, and integrated WAN interface support in one box. |
| Ability to use the network infrastructure for security | Cisco 800, 1800, 2800, and 3800 Series, Cisco 7200, and Cisco ASR 1000 Series | You can load Cisco IOS Firewall on existing Cisco IOS Software-based 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--you can use the same management infrastructure and no additional staff training is required. |
| Extensive VPN and firewall support in a single device | Cisco 800, 1800, 2800, and 3800 Series, Cisco 7200, and Cisco ASR 1000 Series | Deploying Cisco IOS Firewall with Cisco IOS encryption and QoS VPN features facilitates 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. |
| High-performance, highly available WAN headend and Internet edge | Cisco ASR 1000 Series | <p>Turn on embedded, high-performance security services in Cisco ASR 1000 Series without affecting WAN routing performance. An integrated "all-in-one" router approach simplifies operations, reducing costs and the time to qualify, deploy, and maintain the WAN infrastructure.</p> <p>High-Performance, Next-Generation Router for New and Faster WAN Edge Services</p> <ul style="list-style-type: none"> • Up to 20-fold increase in platform performance compared to Cisco 7200 Series • 5- 10- and 20-Gbps firewall, and NAT along with onboard multigigabit IPsec acceleration • High-speed embedded deep packet inspection using NBAR and Flexible Packet Matching (FPM) • Cisco QuantumFlow Processor, the industry's first massive parallel processor hardware and software architecture • Positioned between Cisco 7200 Series and Cisco Catalyst 6500 Series/7600 Series <p>Unparalleled WAN Availability with Carrier-Class Design</p> <ul style="list-style-type: none"> • Control- and data-plane separation for maximum system availability • Redundant control plane for rapid failover with zero packet loss • Redundant forwarding engines with stateful failover for minimal packet loss • Software redundancy with dual Cisco IOS Software images on board • Modular Cisco IOS XE Software for process restartability, fault management, and In Service Software Upgrades (ISSUs) <p>Operational Excellence</p> <ul style="list-style-type: none"> • Optimize WAN costs with bandwidth utilization, network consolidation, service integration, and power efficiency • Increase capacity without forklift upgrade • Scalable and flexible QoS for optimal application performance • Scalable NetFlow v9 |
| Per-subscriber firewall for service provider broadband networks | Cisco ASR 1000 Series | <p>This feature integrates the Cisco IOS Zone-Based Policy Firewall with the Cisco ASR 1000 Series rich broadband feature set to enable Internet service providers to offer firewall services to their broadband subscribers.</p> <p>This solution is centralized on the Cisco ASR 1000 Series as the L2TP Network Server (LNS). All functions are embedded in the QuantumFlow Processor, thus providing multigigabit performance centralized firewall service in broadband environments.</p> <p>Primary features include:</p> <ul style="list-style-type: none"> • Dynamic assignment of virtual access interfaces to firewall zones through RADIUS • Application-level monitoring and stateful packet inspection at the granularity of the subscriber Point-to-Point Protocol (PPP) session • Inclusion of subscriber's username in the firewall drop log message to track drops on per-subscriber basis • Ability to configure zone pairs with matching source and destination zones to control traffic between subscribers |

Table 5. When to Choose Cisco FWSM

| Customer Requirement | Cisco FWSM Benefit |
|--|---|
| Service provider and large enterprise headends and data centers | 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: 5 Gbps throughput; 100,000 cps; and 1 million concurrent connections. You can deploy up to four Cisco FWSMs 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. You can partition a single FWSM into up to 100 virtual firewalls (security contexts). Using the Cisco FWSM Resource Manager, your organization can limit the resources allocated to any security context at any time, helping ensure that one security context does not interfere with another. |
| Ability to use network and switching infrastructure at the headend or data center | You can deploy the Cisco FWSM 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, you can deploy the FWSM 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. |
| High availability | You can deploy the Cisco FWSM in pairs to provide intra- or interchassis stateful failover services that help ensure resilient network protection for the most critical environments. Modules configured in failover mode continuously synchronize their connection state and device configuration data; if a failure occurs, modules fail over with full transparency to users. |

Figure 5 illustrates how you can deploy Cisco integrated firewall solutions 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 in Cisco firewall solutions, Cisco provides integrated security management applications for customers who want to manage more than the few devices for which the embedded managers are designed.

For customers looking for comprehensive security policy administration for Cisco firewall solutions, Cisco provides the Cisco Security Manager. Cisco Security Manager is a powerful but very easy-to-use solution to centrally provision all aspects of device configuration and security policies for Cisco firewalls, VPNs, and intrusion prevention systems (IPSs). The solution effectively manages even small networks consisting of fewer than 10 devices, but also scales to efficiently manage large networks with thousands of devices. Scalability is achieved through intelligent policy-based management techniques that can simplify administration.

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 automitigation capabilities, Cisco Security MARS can identify, manage, and eliminate network attacks and maintain compliance. Cisco Security Manager and Cisco Security MARS are integrated to decrease operating expenses (OpEx) and increase return on investment (ROI) for firewall deployments.

For example, you can expedite trouble-ticket resolution by selecting a firewall syslog event in Cisco Security MARS, which displays the access-list rule in Cisco Security Manager that generated the syslog.

Cisco Services for the Enterprise WAN Edge

Cisco and our partners help make your enterprise WAN edge deployment a success with a broad portfolio of services based on proven methodologies. We can help you establish a secure, resilient WAN architecture and successfully integrate Cisco® Unified Communications, Cisco TelePresence™, security, and mobility technologies with bandwidth to support video, collaboration, branch solutions, and growth in alignment with your business goals. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help maintain operational health, strengthen software application functionality, solve performance issues, and lower expenses. Optimization services are designed to continually improve performance and help your team succeed with new technologies. For more information, visit <http://www.cisco.com/go/services>.

Additional Information

For more information, please visit the following sites:

- Cisco ASA 5500 Series Adaptive Security Appliances: <http://www.cisco.com/go/asa>
- Cisco PIX Security Appliances: <http://www.cisco.com/go/pix>
- Cisco ASR 1000 Series Aggregation Services Routers: <http://www.cisco.com/go/asr1000>
- 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>
- Cisco Security Manager: <http://www.cisco.com/go/csmanager>
- Cisco Security MARS: <http://www.cisco.com/go/mars>
- SAFE Blueprint from Cisco: <http://www.cisco.com/go/safe>



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSF, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0903R)

Printed in USA

C78-345384-08 04/09