DATA SHEET

CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES SOLUTION OVERVIEW

Cisco® ASA 5500 Series adaptive security appliances are purpose-built solutions that combine best-of-breed security and VPN services with the innovative Cisco Adaptive Identification and Mitigation (AIM) architecture. Designed as a key component of the Cisco Self-Defending Network, the Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network security appliance family that provides the security breadth and depth for protecting small and medium-sized business and enterprise networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.

The Cisco ASA 5500 Series delivers a powerful combination of multiple market-proven technologies in a single platform, making it operationally and economically feasible to deploy comprehensive security services to more locations. And its multifunction security profile virtually eliminates the difficult---and risky---decision of making trade-offs between robust security protection and the operational costs associated with multiple devices in numerous locations.

Figure 1. Cisco ASA 5500 Series Adaptive Security Appliance

The Cisco ASA 5500 Series helps businesses more effectively and efficiently protect their networks while delivering exceptional investment protection via the following key elements:

- **Market-proven security and VPN capabilities**---Full-featured, high-performance firewall, intrusion prevention system (IPS), network antivirus, and IP Security/Secure Sockets Layer (IPSec/SSL) VPN technologies deliver robust application security, user- and application-based access control, worm and virus mitigation, malware protection, and remote user/site connectivity.
- **Extensible Adaptive Identification and Mitigation services architecture**---Leveraging a modular services processing and policy framework, AIM enables the application of specific security or network services on a per traffic flow basis, delivering highly granular policy controls and anti-x protection with streamlined traffic processing. The efficiencies of the Cisco ASA 5500 Series AIM architecture, as well as software extensibility and hardware extensibility via user-installable Security Services Modules (SSMs), enable evolution of existing services as well as deployment of new services without requiring a platform replacement or performance compromise. As the architectural foundation of the Cisco ASA 5500 Series, AIM enables highly customizable security policies and unprecedented services extensibility to help protect against the fast evolving threat environment.
- **Reduced deployment and operations costs**---Multifunction appliance allows for platform, configuration, and management standardization, helping to decrease the costs of deployment and ongoing operations.

MARKET-PROVEN SECURITY AND VPN CAPABILITIES

The Cisco ASA 5500 Series leverages Cisco's expertise in developing industry-leading and award-winning security and VPN solutions, and integrates the latest technologies from Cisco PIX® 500 Series Security Appliances, Cisco IPS 4200 Series Intrusion Prevention Systems, and Cisco VPN 3000 Series Concentrators. By combining these technologies, the Cisco ASA 5500 Series delivers an unmatched, best-of-breed solution that stops the broadest range of threats and provides businesses with flexible, secure connectivity options. The breadth and depth of security and networking services provided by the Cisco ASA 5500 Series enable it to protect any area of the network, including the most common threat vectors such as mobile users, remote sites, and unmanaged desktops and servers. As a key component of Cisco's Adaptive Threat Defense and Unified Secure Access strategies, the Cisco ASA 5500 Series converges a wide range of security and VPN technologies to provide rich application security, anti-x defenses, network containment and control, and secure connectivity.

Application Security

The Cisco ASA 5500 Series provides strong application-layer security through 30 intelligent, application-aware inspection engines that examine network flows at Layers 2–7. To defend networks from application-layer attacks and to give businesses control over how applications and protocols are used in their environments, these inspection engines incorporate extensive application and protocol knowledge and employ security enforcement technologies that include application/protocol command filtering, protocol anomaly detection, and application and protocol state tracking. As another layer of application inspection and control, these inspection engines also incorporate attack detection and mitigation techniques such as buffer overflow defenses, content filtering and verification, and URL deobfuscation services. Inspection engines are available for a wide range of popular applications and protocols, including Web services, file transfer services, e-mail services, voice and multimedia services, database services, operating system services, and 3G Mobile Wireless services. These inspection engines also give businesses control over threats such as instant messaging, peer-to-peer file sharing, and other tunneling applications, allowing businesses to enforce usage policies and protect network bandwidth for legitimate business applications.

Anti-X Defenses

The Cisco ASA 5500 Series provides advanced, high-performance protection against network- and application-layer attacks, denial of service (DoS) attacks, and malware, including worms, network viruses, Trojan horses, spyware, and adware. Effective anti-x defense requires broad attack detection coupled with advanced analysis techniques, resulting in highly accurate threat classification that helps ensure appropriate mitigation actions are taken without impact to legitimate network traffic.

Advanced detection techniques---To help ensure that threats do not go unnoticed, the Cisco ASA 5500 Series offers numerous detection methods to detect policy violations, anomalous activity, and vulnerability exploitation. These methods include stateful pattern recognition for stopping attacks hidden inside a data stream; protocol analysis to validate network traffic; traffic anomaly detection to identify attacks that cover multiple sessions and connections; protocol anomaly detection to identify attacks based on observed deviations in the normal RFC behavior of a protocol or service; and Layer 2 analysis to detect man-in-the-middle attacks. Specialized safeguards are used to "scrub" network traffic to prevent "detection evasion" attempts; these safeguards include IP fragmentation reassembly and normalization, TCP stream reassembly and normalization, TCP evasion control, IP antispoofing, and deobfuscation.

Combined with the extensive detection techniques are two innovative analysis and correlation technologies from Cisco Systems that enable accurate mitigation of the detected threats: Risk Rating and the Meta Event Generator.

Risk Rating---To help ensure that malicious attacks are stopped without impact to legitimate traffic, the Cisco ASA 5500 Series makes use of Cisco's innovative Risk Rating technology. Going beyond the typical single factor methods in determining threat risk, Risk Rating incorporates four measures to accurately determine the risk of an event:

- **Event severity**---Rating indicating the relative impact of the threat
- **Signature fidelity**---Rating indicating the accuracy of the signature
- **Asset value**---Customizable value indicating the importance of the attack target (low value for a print server in a wiring closet, a high value for an e-commerce server in a data center, for example)
- **Attack relevancy**---Value based on susceptibility of the target to the attack type

These four factors combine to produce an accurate threat rating that allows for confident mitigation actions to take place.

Meta Event Generator---To quickly and accurately identify and stop worms that can rapidly propagate and cause extensive damage, the Cisco ASA 5500 Series includes Cisco's Meta Event Generator technology, which provides unique on-device correlation capabilities. This is achieved through real-time modeling of worm behavior, including correlation of multiple event types and the time between individual events. As worms attempt to move through a network, they propagate through the transmission of multiple packets, which in many cases appear to be legitimate traffic. The Meta Event Generator uses its real-time correlation services to identify the initial packets associated with worm propagation and stops the follow-on packets necessary to complete the worm infestation. This results in the worm not being able to reach the intended target intact, thereby "killing" the worm.

Network Containment and Control

The Cisco ASA 5500 Series delivers a wide range of network containment and control services to give businesses precise control over application access and network traffic flows. As a secure foundation, Cisco ASA 5500 Series appliances provide rich stateful inspection firewall services, tracking the state of all network communications and preventing unauthorized network access. Businesses can enforce their corporate security policies, as well as application and resource usage policies, using the highly flexible access control services provided by the Cisco ASA 5500 Series. Policies can easily be constructed using a variety of elements, including user identity and group membership, network resource addresses, predefined or custom application types, associated VPN tunnels, time of day, day of week, and more. Ongoing administration of these policies can be simplified using the network and application object grouping capabilities offered by the Cisco ASA 5500 Series, enabling businesses to easily add a new network device or application to an existing object group, resulting in the new device or application having the same policies applied to it as other members of the object group.

Secure Connectivity Services

The Cisco ASA 5500 Series provides robust site-to-site and remote-access VPN services, enabling businesses to create secure connections across public networks to mobile users, remote sites, and business partners. An integrated approach to security is provided, enabling organizations to gain the connectivity and cost benefits of the Internet, without compromising the integrity of the corporate security policy.

By integrating VPN services with the wide range of security services offered by the Cisco ASA 5500 Series, businesses benefit from a stronger, more secure VPN connectivity. Integrated Cisco Adaptive Threat Defense capabilities help ensure that VPNs do not become a conduit for network attacks such as worms, viruses, malware, or hacking. Detailed application and access control policies can also be applied to VPN traffic, so individuals and groups of users only have access to the services and resources to which they are entitled. Additionally, customized quality of service (QoS) policies can be applied on a per-user, per-group, per-tunnel, or per-flow basis, helping to ensure that the appropriate priority and bandwidth restrictions are applied to specific network traffic flows.

Remote-access VPN---The Cisco ASA 5500 Series offers flexible technologies that deliver tailored solutions to suit connectivity requirements, providing employees' company-managed desktops with robust, customizable remote access via an IPSec VPN. For situations where endpoints are not company-managed, such as extranets, Internet kiosks, or employee-owned desktops, the Cisco ASA 5500 Series delivers WebVPN for SSL-based remote access. Taking advantage of Cisco's remote-access expertise, enterprises can deploy a single integrated platform with broad support for core enterprise applications.

- Flexible platform---Offers both IPSec and SSL-based VPN services on a single platform, eliminating the need to provide parallel solutions. The Cisco ASA 5500 Series eliminates the inefficiencies and added costs of deploying separate, distinct platforms for both SSL and IPSec VPNs.
- Resilient clustering---Allows remote-access deployments to scale cost-effectively by evenly distributing VPN sessions across Cisco ASA 5500 Series and VPN 3000 Series platforms without requiring any user intervention. This highly resilient capability eliminates any single point of failure, allows businesses to scale their VPN headends as needed, and provides businesses with excellent investment protection.
- Cisco Easy VPN---Delivers a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture. Cisco ASA 5500 Series appliances dynamically push the latest VPN security policies to remote VPN devices and clients, helping to ensure that those remote endpoints have up-to-date policies in place before the connection is established, thereby offering the ultimate flexibility, scalability, and ease of use. Furthermore, the Cisco ASA 5500 Series provides VPN client software with "auto-update" capabilities that enable automated version upgrades for Cisco VPN Client software operating on remote desktops.

Site-to-site VPN---Using the standards-based site-to-site VPN capabilities provided by the Cisco ASA 5500 Series, businesses can securely extend their networks across low-cost Internet connections to business partners and remote and satellite offices worldwide.

- VPN infrastructure for today's applications---The Cisco ASA 5500 Series provides a VPN infrastructure capable of converged voice, video, and data across a secure IPSec network, by combining robust site-to-site VPN support with rich inspection capabilities, QoS, dynamic routing, and stateful failover features, allowing businesses to take advantages of the many benefits of converged networks.
- Robust security and performance---Branch and remote offices extend a company's reach into important markets and locations. Cisco ASA 5500 Series-based VPN solutions enable secure, high-speed communications between multiple locations, offering the performance, reliability, and availability that businesses need to communicate.

Intelligent Network Integration

The Cisco ASA 5500 Series takes advantage of more than 20 years of Cisco networking leadership and innovation, and delivers a wide range of intelligent networking services for seamless integration into today's diverse network environments. Key network integration capabilities include:

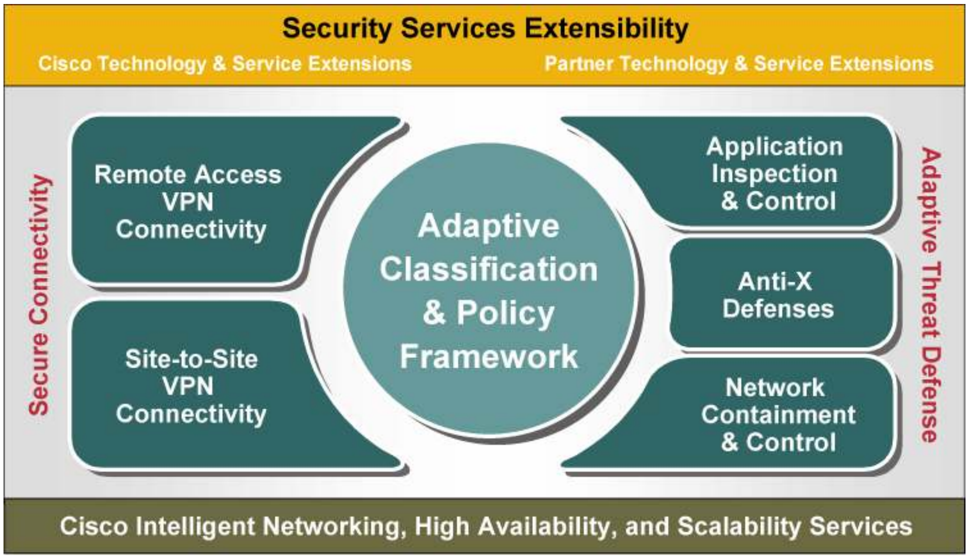
- Layer 2 transparent firewall---Provides the ability to rapidly deploy Cisco ASA 5500 Series appliances into existing networks without requiring any addressing changes. Delivers high-performance stealth Layers 2–7 security services and provides protection against network-layer attacks with integration in complex routing, high availability, and multicast environments.
- Services virtualization---Enables the logical partitioning of a single Cisco ASA 5500 Series appliance into multiple virtual firewalls, each with its own unique policies and administration. This capability is ideal for enterprises consolidating multiple firewalls into a single Cisco ASA 5500 Series appliance, or for service providers that offer managed firewall or hosting services.
- 802.1q-based VLAN support---Provides easy integration into switched network environments.
- Open Shortest Path First (OSPF) dynamic routing services---Improve networking resiliency by detecting network outages within seconds, and routing around them.
- Protocol-Independent Multicast (PIM) Sparse Mode v2 and bidirectional PIM routing support---Provide secure delivery of mission-critical real-time enterprise applications, collaborative computing applications, and streaming multimedia services.
- IPv6 support---Allows secure deployment of next-generation IPv6 networks.
- Quality of Service (QoS)---Low-Latency Queuing (LLQ) and Traffic Policing features support applications with demanding QoS requirements, such as voice or video, helping to ensure an end-to-end network QoS policy. Latency-sensitive traffic can be prioritized ahead of file transfer and other more delay-tolerant traffic.
- IP phone "zero-touch provisioning" services---Simplifies IP phone deployments by helping the phones register with the correct Cisco CallManager systems and download any additional configuration information and software images.

- Resilient architecture---Provides businesses with both stateful Active/Active and Active/Standby high-availability services, as well as VPN device clustering, to help maximize throughput and network uptime. The Cisco ASA 5500 Series also supports “zero-downtime software upgrades,” which allow businesses to install software maintenance releases on failover pairs without affecting connections or network uptime. Additionally, integrated dynamic load-balancing capabilities provide high session scalability and resiliency for remote-access VPN deployments.

UNIQUE ADAPTIVE IDENTIFICATION AND MITIGATION SERVICES ARCHITECTURE

Through its unique Adaptive Identification and Mitigation services architecture, the Cisco ASA 5500 Series brings a new level of security and policy control to networks (Figure 2). The AIM architecture allows businesses to adapt and extend the security services profile of the Cisco ASA 5500 Series through highly customizable flow-specific security policies that tailor security needs to application requirements while providing performance and security service extensibility via user-installable security services modules (SSMs). This adaptable architecture enables businesses to deploy security services when and where they are needed, such as tailoring inspection techniques to specific application and user needs or adding additional intrusion prevention and anti-x services such as those delivered by the Adaptive Inspection and Prevention Security Services Module (AIP SSM). Furthermore, the AIM architecture enables the integration of future threat identification and mitigation services, further extending the outstanding investment protection provided by the Cisco ASA 5500 Series, and allowing businesses to adapt their network defenses to new threats as they arise.

Figure 2. Cisco Adaptive Identification and Mitigation services architecture

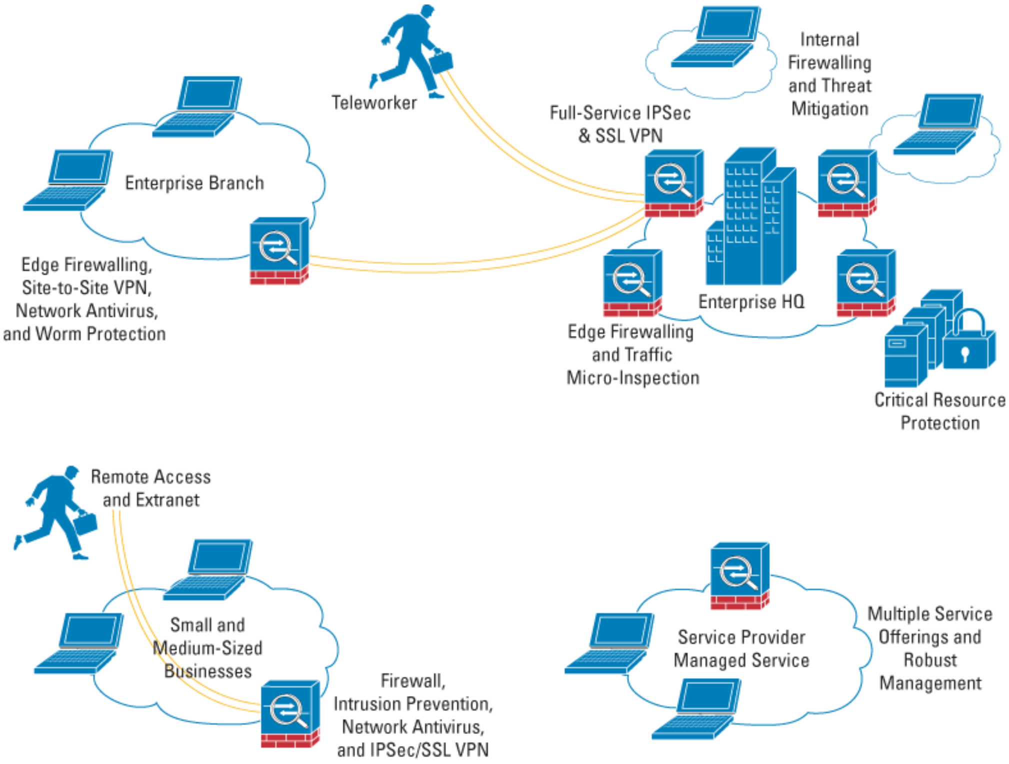

Security Services Extensibility
Cisco Technology & Service Extensions
Partner Technology & Service Extensions
Secure Connectivity
Remote Access VPN Connectivity
Site-to-Site VPN Connectivity
Adaptive Classification & Policy Framework
Application Inspection & Control
Anti-X Defenses
Network Containment & Control
Adaptive Threat Defense
Cisco Intelligent Networking, High Availability, and Scalability Services

Using the powerful policy framework offered by the Cisco ASA 5500 Series, administrators can orchestrate detailed policies that define what specific services are applied to individual traffic flows. Services include more than 30 different application- and protocol-specific inspection engines, QoS policies, anti-x services, and other inspection and network services. Policies can be based on numerous criteria, including network addresses, traffic types, VPN tunnel, and application or destination target. By enabling the selection of specific security or network services on a per-flow basis, this architecture allows security services to be implemented in a highly granular fashion in support of specific security policies.

REDUCED DEPLOYMENT AND OPERATIONS COSTS

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, providing platform and management standardization. It can be deployed as a converged threat prevention device by using its access control, application inspection, and worm, virus, and other malware mitigation technologies. It can be used as a dedicated VPN termination device by using its highly scalable site-to-site IPSec and SSL remote-access 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 that internal users may unwittingly bring into a network. In small business and branch office environments, the Cisco ASA 5500 Series serves as an “all-in-one” solution, offering comprehensive threat prevention and VPN services better suiting the budgets and operational models of such deployments. This adaptive “single platform, many uses” approach reduces the number of platforms that must be deployed and managed. This common operating environment also simplifies configuration, monitoring, troubleshooting, and security staff training. To further minimize operations costs, the Cisco ASA 5500 Series is highly network-aware---it can be inserted gracefully into the network without disrupting legitimate traffic and applications.

Figure 3. Cisco ASA 5500 Series Deployment Examples


Teleworker
Internal Firewalling and Threat Mitigation
Full-Service IPSec & SSL VPN
Enterprise Branch
Edge Firewalling, Site-to-Site VPN, Network Antivirus, and Worm Protection
Enterprise HQ
Edge Firewalling and Traffic Micro-Inspection
Critical Resource Protection
Remote Access and Extranet
Small and Medium-Sized Businesses
Firewall, Intrusion Prevention, Network Antivirus, and IPSec/SSL VPN
Service Provider Managed Service
Multiple Service Offerings and Robust Management

APPLIANCE MODELS

The Cisco ASA 5500 Series delivers solutions for environments ranging from small and medium-sized businesses to large enterprises through the Cisco ASA 5510, 5520, and 5540 appliances. Table 1 displays performance capacities and capabilities of each of these models.

Table 1. Appliance Models

Cisco ASA 5500 Series Adaptive Security Appliance Models	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540
Firewall Throughput	Up to 300 Mbps	Up to 450 Mbps	Up to 650 Mbps
Concurrent Threat Mitigation Throughput (Firewall + Anti-x Services)	Up to 150 Mbps, with AIP-SSM-10	Up to 375 Mbps, with AIP-SSM-20	Up to 450 Mbps, with AIP-SSM-20
3DES/AES VPN Throughput	Up to 170 Mbps	Up to 225 Mbps	Up to 325 Mbps
Connections	32,000/64,000*	130,000	280,000
IPSec VPN Peers	50/150*	300/750*	500/2000*/5000*
WebVPN Peers	50/150*	300/750*	500/1250*/2500*
Integrated I/O Ports	3 Fast Ethernet + 1 management/5 Fast Ethernet*	4 Gigabit Ethernet + 1 Fast Ethernet	4 Gigabit Ethernet + 1 Fast Ethernet
Virtual Interfaces (VLANs)	0/10*	25	100
Security Contexts	Not supported	Up to 10*	Up to 50*
High Availability/Scalability	Not supported / Active/Standby*	Active/Active, Active/Standby, VPN clustering/load balancing	Active/Active, Active/Standby, VPN clustering/load balancing

* Available through an upgrade license.

For complete specifications and more information about these platforms, please see the Cisco ASA 5500 Series data sheet.

ORDERING INFORMATION

Table 2 provides ordering information for Cisco ASA 5500 Series appliances. To place an order, visit the Cisco Ordering Home Page.

Table 2. Ordering Information

Product Name	Part Number
Cisco ASA 5510 Appliance (3 Fast Ethernet, 50 VPN peers, Triple Data Encryption Standard/Advanced Encryption Standard [3DES/AES])	ASA5510-BUN-K9
Cisco ASA 5510 Appliance with AIP-SSM-10 (3 Fast Ethernet, 50 VPN peers, AIP-SSM-10, 3DES/AES)	ASA5510-AIP10-K9
Cisco ASA 5510 Security Plus Appliance (5 Fast Ethernet, 150 VPN peers, 3DES/AES)	ASA5510-SEC-BUN-K9
Cisco ASA 5520 Appliance (4 Gigabit Ethernet + 1 Fast Ethernet, 300 VPN peers, 3DES/AES)	ASA5520-BUN-K9
Cisco ASA 5520 Appliance with AIP-SSM-10 (4 Gigabit Ethernet + 1 Fast Ethernet, 300 VPN peers, AIP-SSM-10, 3DES/AES)	ASA5520-AIP10-K9
Cisco ASA 5520 Appliance with AIP-SSM-20 (4 Gigabit Ethernet + 1 Fast Ethernet, 300 VPN peers, AIP-SSM-20, 3DES/AES)	ASA5520-AIP20-K9
Cisco ASA 5540 Appliance (4 Gigabit Ethernet + 1 Fast Ethernet, 500 VPN peers, 3DES/AES)	ASA5540-BUN-K9
Cisco ASA 5540 Appliance with AIP-SSM-20 (4 Gigabit Ethernet + 1 Fast Ethernet, 500 VPN peers, AIP-SSM-20, 3DES/AES)	ASA5540-AIP20-K9

For a complete list of all product part numbers, please see the Cisco ASA 5500 Series data sheet.

SERVICE AND SUPPORT

Cisco offers a wide range of services programs to accelerate customer success. These innovative service programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see Cisco Technical Support Services and Cisco Advanced Services; for services specific to IPS features delivered via the AIP-SSM, see Cisco Services for IPS.

FOR MORE INFORMATION

For more information, please visit the following links:

Cisco ASA 5500 Series: http://www.cisco.com/go/asa

Cisco Adaptive Security Device Manager: http://www.cisco.com/go/asdm

Cisco Product Certifications: http://www.cisco.com/go/securitycert

Cisco Technical Support Services: http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

Cisco Advanced Services: http://www.cisco.com/en/US/products/svcs/ps11/services_segment_category_home.html

Cisco Services for IPS: http://www.cisco.com/en/US/products/ps6076/serv_home.html

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA