Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Module

The Cisco® Advanced Inspection and Prevention Security Services Module (AIP-SSM) for the Cisco ASA 5500 Series Adaptive Security Appliance provides proactive, full-featured intrusion prevention services to stop malicious traffic, including worms and network viruses, before they can affect your network.

Security Services Module

Providing unparalleled protection for an organization's critical information assets, the Cisco ASA 5500 Series Adaptive Security Appliance provides best-in-class firewall and VPN capabilities in a single, easy-to-deploy platform. When combined with the advanced inspection capabilities of the AIP-SSM, the Cisco ASA 5500 Series Adaptive Security Appliance provides integrated, converged protection of an organization's servers and infrastructure without compromising the ability to use the network as a business tool.

AIP-SSM Intrusion Prevention Services

Cisco AIP-SSM combines inline prevention services with innovative technologies to improve accuracy. The result is total confidence in the protection offered by your intrusion prevention system (IPS) solution, without the fear of legitimate traffic being dropped. When deployed within Cisco ASA 5500 Series appliances, the AIP-SSM offers comprehensive protection of your network by collaborating with other network security resources, providing a proactive approach to protecting your network.

The Cisco AIP SSM helps users stop threats with greater confidence through the use of:

- **Accurate inline prevention technologies**—Provides unparalleled ability to take preventive action against a broader range of threats without the risk of dropping legitimate traffic. These unique technologies offer intelligent, automated, contextual analysis of your data and help ensure you are getting the most out of your intrusion prevention solution.

- **Multivector threat identification**—Protects your network from policy violations, vulnerability exploitations, and anomalous activity through detailed inspection of traffic in Layers 2 through 7.

- **Unique network collaboration**—Enhances scalability and resiliency through network collaboration, including efficient traffic capture techniques, load-balancing capabilities, and visibility into encrypted traffic.

- **Powerful management, event correlation, and support services**—Enables a complete solution, including configuration, management, data correlation, and advanced support services. In particular, the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) identifies, isolates, and recommends precision removal of offending elements, for a networkwide intrusion prevention solution. And the Cisco Incident Control System (ICS) prevents new worm and virus outbreaks by enabling the network to rapidly adapt and provide a distributed response.

When combined, these elements provide a comprehensive inline prevention solution, giving you the confidence to detect and stop the broadest range of malicious traffic before your business continuity is affected.

Table 1. Cisco ASA AIP SSM-10, Cisco ASA AIP SSM-20, Cisco ASA AIP SSM-40

Feature	Cisco ASA AIP SSM-10	Cisco ASA AIP SSM-20	Cisco ASA AIP SSM 40
Concurrent Threat Mitigation Throughput (Firewall and IPS Services)	• 150 Mbps with Cisco ASA 5510 • 225 Mbps with Cisco ASA 5520	• 375 Mbps with Cisco ASA 5520 • 500 Mbps with Cisco ASA 5540	• 450 Mbps with Cisco ASA 5520 • 650 Mbps with Cisco ASA 5540
Technical Specifications			
Memory	1 GB	2 GB	4 GB
Flash	256 MB	256 MB	2 GB
Environmental Operating Ranges			
Operating			
Temperature	32 to 104ºF (0 to 40ºC)		
Relative Humidity	5 to 95 percent noncondensing		
Nonoperating			
Temperature	-13 to 158ºF (-25 to 70ºC)		
Power Consumption	90W maximum		
Physical Specifications			
Dimensions (H x W x D)	1.70 x 6.80 x 11.00 in. (4.32cm x 17.27cm x 27.94cm)		
Weight (with Power Supply)	3.00 lb (1.36 kg)		2.58 lb (1.17 kg)
Regulatory and Standards Compliance			
Safety	UL 1950, CSA C22.2 No. 950, EN 60950 IEC 60950, AS/NZS3260, TS001		
Electromagnetic Compatibility (EMC)	CE marking, FCC Part 15 Class A, AS/NZS 3548 Class A, VCCI Class A, EN55022 Class A, CISPR22 Class A, EN61000-3-2, EN61000-3-3		

Ordering Information

To place an order, visit the [Cisco Ordering Home Page](#). See Table 2 for ordering information.

Table 2. Ordering Information

Product Name	Part Number
Cisco ASA 5510 Series Adaptive Security Appliances	
Cisco ASA 5510 Adaptive Security Appliance with SSM-AIP-10 (chassis, software, 50 VPN peers, 4 Fast Ethernet interfaces, Triple Data Encryption Standard/Advanced Encryption Standard [3DES/AES])	ASA5510-AIP10-K9
Cisco ASA 5520 Series Adaptive Security Appliances	
Cisco ASA 5520 Adaptive Security Appliance with SSM-AIP-10 (chassis, software, 300 VPN peers, 4 Gigabit Ethernet interfaces, 3DES/AES)	ASA5520-AIP10-K9
Cisco ASA 5520 Adaptive Security Appliance with SSM-AIP-20 (chassis, software, 300 VPN peers, 4 Gigabit Ethernet interfaces, 3DES/AES)	ASA5520-AIP20-K9
Cisco ASA 5520 Adaptive Security Appliance with SSM-AIP-40 (chassis, software, 300 VPN peers, 4 Gigabit Ethernet interfaces, 3DES/AES)	ASA5520-AIP40-K9

Product Name	Part Number
Cisco ASA 5540 Series Adaptive Security Appliances	
Cisco ASA 5540 Adaptive Security Appliance with SSM-AIP-20 (chassis, software, 500 VPN peers, 4 Gigabit Ethernet interfaces, 3DES/AES)	ASA5540-AIP20-K9
Cisco ASA 5540 Adaptive Security Appliance with SSM-AIP-40 (chassis, software, 500 VPN peers, 4 Gigabit Ethernet interfaces, 3DES/AES)	ASA5540-AIP40-K9
Security Services Modules	
Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Module 10 (AIP-SSM-10)	ASA-SSM-AIP-10-K9=
Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Module 20 (AIP-SSM-20)	ASA-SSM-AIP-20-K9=
Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Module 40 (AIP-SSM-40)	ASA-SSM-AIP-40-K9=

Service and Support

Cisco takes a lifecycle approach to services, and with its partners, provides a broad portfolio of Security Services so enterprises can design, implement, operate and optimize network platforms that defend critical business processes against attack and disruption, protect privacy, and support policy and regulatory compliance controls.

Cisco services help you 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, refer to http://www.cisco.com/go/services/security.

The following Cisco Security Services support and compliment the SSM-AIP modules and the ASA 5500 series Adaptive Security Appliances:

Cisco Services for IPS

Cisco Services for IPS helps protect your business against security vulnerabilities by providing hardware and software support, operating system and application updates, access to Cisco security engineering specialists, and timely alerts about late-breaking viruses, worms, and other threats.

Cisco Services for IPS features:

- Signature file updates and alerts
- Registered access to Cisco.com for online tools and technical assistance
- Access to Cisco Technical Assistance Center (TAC)
- Cisco IPS Sensor Software updates
- Options for Advance replacement of failed hardware

Cisco Security Center

The Cisco Security Center provides one-stop shopping for early-warning threat intelligence threat and vulnerability analysis, Cisco IPS Signatures and mitigation techniques. Visit and bookmark the Cisco Security Center at: http://www.cisco.com/security

Cisco Security Intellishield Alert Manager

Cisco Security Intellishield Alert Manager Service provides a customizable, web-based threat and vulnerability alert service that allows organizations to easily access timely, accurate and credible information about potential vulnerabilities in their environment.

Cisco Security Optimization Service

Cisco Security Optimization Service—increasingly the network infrastructure is the foundation of the agile and adaptive business. The Cisco Security Optimization Service supports the continuously evolving security system to meet ever-changing security threats, through a combination of planning and assessments, design, performance tuning, and ongoing support for system changes and helps integrate security into the core network infrastructure.

Table 3. Ordering Information for Cisco Services for IPS

Appliance/Module Part Number	Service Option Part Number	Service Option Name
ASA5510-AIP10-K9	• CON-SU1-AS1A10K9 • CON-SU2-AS1A10K9 • CON-SU3-AS1A10K9 • CON-SU4-AS1A10K9 • CON-SUO1-AS1A10K9 • CON-SUO2-AS1A10K9 • CON-SUO3-AS1A10K9 • CON-SUO4-AS1A10K9	• IPS Service with Advance Hardware replacement Next Business Day (NBD) • IPS Svc with Adv HW repl 8x5 within four hours • IPS Svc with Adv HW repl 24x7 within four hours • IPS Svc with Adv HW repl 24x7 within two hours • IPS Svc with Adv HW repl and Field Engineer onsite NBD • IPS Svc with Adv HW repl onsite 8x5x4 • IPS Svc with Adv HW repl onsite 24x7x4 • IPS Svc with Adv HW repl onsite 24x7x2
ASA5520-AIP10-K9	• CON-SU1-AS2A10K9 • CON-SU2-AS2A10K9 • CON-SU3-AS2A10K9 • CON-SU4-AS2A10K9 • CON-SUO1-AS2A10K9 • CON-SUO2-AS2A10K9 • CON-SUO3-AS2A10K9 • CON-SUO4-AS2A10K9	• IPS Svc with Adv HW repl NBD • IPS Svc with Adv HW repl 8x5x4 • IPS Svc with Adv HW repl 24x7x4 • IPS Svc with Adv HW repl 24x7x2 • IPS Svc with Adv HW repl onsite NBD • IPS Svc with Adv HW repl onsite 8x5x4 • IPS Svc with Adv HW repl onsite 24x7x4 • IPS Svc with Adv HW repl onsite 24x7x2
ASA5520-AIP20-K9	• CON-SU1-AS2A20K9 • CON-SU2-AS2A20K9 • CON-SU3-AS2A20K9 • CON-SU4-AS2A20K9 • CON-SUO1-AS2A20K9 • CON-SUO2-AS2A20K9 • CON-SUO3-AS2A20K9 • CON-SUO4-AS2A20K9	• IPS Svc with Adv HW repl NBD • IPS Svc with Adv HW repl 8x5x4 • IPS Svc with Adv HW repl 24x7x4 • IPS Svc with Adv HW repl 24x7x2 • IPS Svc with Adv HW repl onsite NBD • IPS Svc with Adv HW repl onsite 8x5x4 • IPS Svc with Adv HW repl onsite 24x7x4 • IPS Svc with Adv HW repl onsite 24x7x2
ASA5520-AIP40-K9	• CON-SU1-AS2A40K9 • CON-SU2-AS2A40K9 • CON-SU3-AS2A40K9 • CON-SU4-AS2A40K9 • CON-SUO1-AS2A40K9 • CON-SUO2-AS2A40K9 • CON-SUO3-AS2A40K9 • CON-SUO4-AS2A40K9	• IPS Svc with Adv HW repl NBD • IPS Svc with Adv HW repl 8x5x4 • IPS Svc with Adv HW repl 24x7x4 • IPS Svc with Adv HW repl 24x7x4 • IPS Svc with Adv HW repl onsite NBD • IPS Svc with Adv HW repl onsite 8x5x4 • IPS Svc with Adv HW repl onsite 24x7x4 • IPS Svc with Adv HW repl onsite 24x7x2

Appliance/Module Part Number	Service Option Part Number	Service Option Name
ASA5540-AIP20-K9	• CON-SU1-AS4A20K9 • CON-SU2-AS4A20K9 • CON-SU3-AS4A20K9 • CON-SU4-AS4A20K9 • CON-SUO1-AS4A20K9 • CON-SUO2-AS4A20K9 • CON-SUO3-AS4A20K9 • CON-SUO4-AS4A20K9	• IPS Svc with Adv HW repl NBD • IPS Svc with Adv HW repl 8x5x4 • IPS Svc with Adv HW repl 24x7x4 • IPS Svc with Adv HW repl 24x7x2 • IPS Svc with Adv HW repl onsite NBD • IPS Svc with Adv HW repl onsite 8x5x4 • IPS Svc with Adv HW repl onsite 24x7x4 • IPS Svc with Adv HW repl onsite 24x7x2
ASA5540-AIP40-K9	• CON-SU1-AS4A40K9 • CON-SU2-AS4A40K9 • CON-SU3-AS4A40K9 • CON-SU4-AS4A40K9 • CON-SUO1-AS4A40K9 • CON-SUO2-AS4A40K9 • CON-SUO3-AS4A40K9 • CON-SUO4-AS4A40K9	• IPS Svc with Adv HW repl NBD • IPS Svc with Adv HW repl 8x5 within four hours • IPS Svc with Adv HW repl 24x7 within four hours • IPS Svc with Adv HW repl 24x7 within two hours • IPS Svc with Adv HW repl onsite NBD • IPS Svc with Adv HW repl onsite 8x5x4 • IPS Svc with Adv HW repl onsite 24x7x4 • IPS Svc with Adv HW repl onsite 24x7x2
ASA-SSM-AIP-10-K9=	• CON-SU1-ASIP10K9 • CON-SU2-ASIP10K9 • CON-SU3-ASIP10K9 • CON-SU4-ASIP10K9 • CON-SUO1-ASIP10K9 • CON-SUO2-ASIP10K9 • CON-SUO3-ASIP10K9 • CON-SUO4-ASIP10K9	• IPS Svc with Adv HW repl NBD • IPS Svc with Adv HW repl 8x5 within four hours • IPS Svc with Adv HW repl 24x7 within four hours • IPS Svc with Adv HW repl 24x7 within two hours • IPS Svc with Adv HW repl onsite NBD • IPS Svc with Adv HW repl onsite 8x5x4 • IPS Svc with Adv HW repl onsite 24x7x4 • IPS Svc with Adv HW repl onsite 24x7x2
ASA-SSM-AIP-20-K9=	• CON-SU1-ASIP20K9 • CON-SU2-ASIP20K9 • CON-SU3-ASIP20K9 • CON-SU4-ASIP20K9 • CON-SUO1-ASIP20K9 • CON-SUO2-ASIP20K9 • CON-SUO3-ASIP20K9 • CON-SUO4-ASIP20K9	• IPS Svc with Adv HW repl NBD • IPS Svc with Adv HW repl 8x5 within four hours • IPS Svc with Adv HW repl 24x7 within four hours • IPS Svc with Adv HW repl 24x7 within two hours • IPS Svc with Adv HW repl onsite NBD • IPS Svc with Adv HW repl onsite 8x5x4 • IPS Svc with Adv HW repl onsite 24x7x4 • IPS Svc with Adv HW repl onsite 24x7x2
ASA-SSM-AIP-40-K9=	• CON-SU1- ASIP40K9 • CON-SU2-ASIP40K9 • CON-SU3-ASIP40K9 • CON-SU4-ASIP40K9 • CON-SUO1-ASIP40K9 • CON-SUO2-ASIP40K9 • CON-SUO3-ASIP40K9 • CON-SUO4-ASIP40K9	• IPS Svc with Adv HW repl NBD • IPS Svc with Adv HW repl 8x5 within four hours • IPS Svc with Adv HW repl 24x7 within four hours • IPS Svc with Adv HW repl 24x7 within two hours • IPS Svc with Adv HW repl onsite NBD • IPS Svc with Adv HW repl onsite 8x5x4 • IPS Svc with Adv HW repl onsite 24x7x4 • IPS Svc with Adv HW repl onsite 24x7x2

For more information on Cisco Services for IPS, please visit
http://www.cisco.com/en/US/products/ps6076/serv_group_home.html.

Export Considerations

Cisco IPS 4200 Series sensors are subject to export controls. For guidance, please refer to the export compliance Website at http://www.cisco.com/wwl/export/crypto/.

For specific export questions, contact export@cisco.com.

Additional Information

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

For more information about Cisco ASA 5500 Series adaptive security appliances, visit http://www.cisco.com/go/asa.

For information about Cisco IDS 4200 Series sensors that have reached end-of-sale status, visit http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_eol_notices_list.html.

For more information about CiscoWorks VPN/Security Management System (VMS) solutions (IPS management) and Cisco Security MARS, visit:

- http://www.cisco.com/go/vms
- http://www.cisco.com/go/mars

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.

Printed in USA

C78-468816-01   06/08