

Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Module and Card

As mobile devices and Web 2.0 applications proliferate, it becomes harder to secure corporate perimeters. A key component of Cisco Secure Borderless Network architecture, the Cisco® Advanced Inspection and Prevention Security Services Module (AIP SSM) with Global Correlation and the Cisco Advanced Inspection and Prevention Security Services Card (AIP SSC) for the Cisco ASA 5500 Series Adaptive Security Appliance provide proactive, full-featured intrusion prevention services to stop malicious traffic before it can affect your network. Cisco Intrusion Prevention System (IPS) with Global Correlation increases the efficacy of traditional IPS. With updates every 5 minutes, Cisco IPS with Global Correlation provides fast and accurate threat protection with real-time global intelligence from Cisco IPS, firewall, email, and web appliances.

The Cisco AIP SSM and AIP SSC are part of the Cisco ASA 5500 Series Adaptive Security Appliance solution, which provides superior firewall and VPN capabilities in a single, easy-to-deploy platform. With the advanced inspection capabilities of the Cisco AIP SSM or Cisco AIP SSC, this appliance provides integrated, converged protection of your servers and infrastructure without compromising your ability to use the network as a business tool.

Cisco AIP SSM Intrusion Prevention Services

The Cisco AIP SSM and AIP SSC combine inline prevention services with innovative technologies to improve accuracy. For you, this means confidence in the protection offered by your IPS solution without the fear of legitimate traffic being dropped. When deployed within Cisco ASA 5500 Series appliances, the AIP SSM and AIP SSC offer comprehensive protection of your IPv6 and IPv4 networks by collaborating with other network security resources, providing a proactive approach to protecting your network.





The Cisco AIP SSM and AIP SSC help you stop threats with greater confidence through the use of:

- **Wide-ranging IPS capabilities:** The Cisco AIP SSM delivers all the IPS capabilities available on Cisco IPS 4200 Series Sensors. The Cisco AIP SSM can be deployed inline in the traffic path or in promiscuous mode, whereby a copy of the traffic is sent to the Cisco AIP SSM for inspection.
- **Global Correlation:** The Cisco AIP SSM provides real-time updates on the global threat environment beyond your perimeter by adding reputation analysis, reducing the window of threat exposure, and providing continuous feedback. With these new capabilities, the Cisco AIP SSM can detect more threats, detect them earlier and more accurately, and protect critical assets from malicious attacks. Global Correlation is available only on the AIP SSM.
- **Comprehensive and timely attack protection:** The Cisco AIP SSM and AIP SSC deliver protection against tens of thousands of known exploits and millions more potential unknown exploit variants using specialized IPS detection engines and thousands of signatures. Cisco Services for IPS provides signature updates through a global intelligence team working 24 hours a day to help ensure that you are protected against the latest threats.
- **Day-zero attack protection:** The Cisco AIP SSM provides powerful protection against day-zero attacks. Cisco anomaly detection learns the normal behavior on your network and alerts you when it sees anomalous activities in your network. Cisco anomaly protection helps protect you against new threats even before signatures are available. Anomaly detection is not available on the AIP SSC.

- **Wireless protection:** The Cisco ASA SSM and AIP SSC are tightly integrated with the Cisco Wireless LAN Controller to help keep intruders out of your wireless network. The Cisco Wireless LAN Controller blocks intruders based on real-time threat intelligence from the Cisco ASA AIP SSM and AIP SSC.

When combined, these elements provide a comprehensive intrusion prevention solution, giving you the confidence to detect and stop malicious traffic before your business continuity is affected. See more features in Table 1.

Table 1. Cisco ASA AIP SSC-5, Cisco ASA AIP SSM-10, Cisco ASA AIP SSM-20, Cisco ASA AIP SSM-40

Feature	Cisco ASA AIP SSC-5	Cisco ASA AIP SSM-10	Cisco ASA AIP SSM-20	Cisco ASA AIP SSM-40
				
Concurrent threat mitigation throughput (firewall and IPS services)	<ul style="list-style-type: none"> • 75 Mbps with Cisco ASA 5505 	<ul style="list-style-type: none"> • 150 Mbps with Cisco ASA 5510 • 225 Mbps with Cisco ASA 5520 	<ul style="list-style-type: none"> • 375 Mbps with Cisco ASA 5520 • 500 Mbps with Cisco ASA 5540 	<ul style="list-style-type: none"> • 450 Mbps with Cisco ASA 5520 • 650 Mbps with Cisco ASA 5540
Global Correlation support	<ul style="list-style-type: none"> • No 	<ul style="list-style-type: none"> • Yes 	<ul style="list-style-type: none"> • Yes 	<ul style="list-style-type: none"> • Yes
Threat protection	<ul style="list-style-type: none"> • 25,000+ threats 	<ul style="list-style-type: none"> • 25,000+ threats 	<ul style="list-style-type: none"> • 25,000+ threats 	<ul style="list-style-type: none"> • 25,000+ threats
Day-zero protection with anomaly detection	<ul style="list-style-type: none"> • No 	<ul style="list-style-type: none"> • Yes 	<ul style="list-style-type: none"> • Yes 	<ul style="list-style-type: none"> • Yes
Custom signature support	<ul style="list-style-type: none"> • No 	<ul style="list-style-type: none"> • Yes 	<ul style="list-style-type: none"> • Yes 	<ul style="list-style-type: none"> • Yes
Virtual sensors	<ul style="list-style-type: none"> • 1 	<ul style="list-style-type: none"> • 4 	<ul style="list-style-type: none"> • 4 	<ul style="list-style-type: none"> • 4
Technical Specifications				
Memory	512 MB	1 GB	2 GB	4 GB
Flash	512 MB	256 MB	256 MB	2 GB
Environmental Operating Ranges				
Operating				
Temperature	32 to 104°F (0 to 40°C)			
Relative humidity	5 to 95 percent noncondensing			
Nonoperating				
Temperature	-13 to 158°F (-25 to 70°C)			
Power consumption	90W maximum			
Physical specifications				
Dimensions (H x W x D)	0.68 x 3.55 x 5.2 in (1.73x9.02x13.21 cm)		1.70 x 6.80 x 11.00 in. (4.32 x 17.27 x 27.94 cm)	
Weight (with power supply)	0.42 lb (0.19 kg)	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 5505 Series Adaptive Security Appliances	
Cisco ASA 5505 50-User Adaptive Security Appliance with AIP-SSC-5 (chassis, software, 8 Fast Ethernet interfaces, 10 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license)	ASA5505-50-AIP5-K9
Cisco ASA 5505 Unlimited-User Adaptive Security Appliance with Security Plus License and AIP-SSC-5 (chassis, software, 8 Fast Ethernet interfaces, 25 IPsec VPN peers, 2 SSL VPN peers, DMZ support, stateless Active/Standby high availability, 3DES/AES license)	ASA5505-U-AIP5P-K9
Cisco ASA 5510 Series Adaptive Security Appliances	
Cisco ASA 5510 Adaptive Security Appliance with AIP-SSM-10 (chassis, software, 250 VPN peers, 4 Fast Ethernet interfaces, Triple Data Encryption Standard/Advanced Encryption Standard [3DES/AES])	ASA5510-AIP10-K9
Cisco ASA 5510 Adaptive Security Appliance with Security Plus License and AIP-SSM-10 (chassis, software, 2 Gigabit Ethernet interfaces, 3 Fast Ethernet interfaces, 250 IPsec VPN peers, 2 SSL VPN peers, Active/Active high availability, 3DES/AES)	ASA5510-AIP10SP-K9
Cisco ASA 5510 Adaptive Security Appliance with Security Plus License and AIP-SSM-20 (chassis, software, 2 Gigabit Ethernet interfaces, 3 Fast Ethernet interfaces, 250 IPsec VPN peers, 2 SSL VPN peers, Active/Active high availability, 3DES/AES)	ASA5510-AIP20SP-K9
Cisco ASA 5520 Series Adaptive Security Appliances	
Cisco ASA 5520 Adaptive Security Appliance with AIP-SSM-10 (chassis, software, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 3DES/AES)	ASA5520-AIP10-K9
Cisco ASA 5520 Adaptive Security Appliance with AIP-SSM-20 (chassis, software, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 3DES/AES)	ASA5520-AIP20-K9
Cisco ASA 5520 Adaptive Security Appliance with AIP-SSM-40 (chassis, software, 750 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 3DES/AES)	ASA5520-AIP40-K9
Cisco ASA 5540 Series Adaptive Security Appliances	
Cisco ASA 5540 Adaptive Security Appliance with AIP-SSM-20 (chassis, software, 5000 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 3DES/AES)	ASA5540-AIP20-K9
Cisco ASA 5540 Adaptive Security Appliance with AIP-SSM-40 (chassis, software, 5000 IPsec VPN peers, 2 SSL VPN peers, 4 Gigabit Ethernet interfaces, 3DES/AES)	ASA5540-AIP40-K9
Security Services Modules and Cards	
Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Card 5 (AIP-SSC-5)	ASA-SSC-AIP-5-K9=
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 you 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, visit <http://www.cisco.com/go/services/security>.

The following Cisco Security Services support and complement the AIP SSM modules and the ASA 5500 Series Adaptive Security Appliances:

Cisco Services for IPS

Cisco Services for IPS provides 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. It features:

- Signature file updates and alerts
- Registered access to Cisco.com for online tools and technical assistance

- Access to Cisco Technical Assistance Center
- 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 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 you to easily access timely, accurate, and credible information about potential vulnerabilities in your environment.

Cisco Security Optimization Service

The Cisco Security Optimization Service supports your 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.

For more information on Cisco Services for IPS, visit

http://www.cisco.com/en/US/products/ps6076/serv_group_home.html.

Additional Information

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

For more information about the Cisco ASA 5500 Series Adaptive Security Appliance, 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.



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, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDR, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco 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. (1002R)