

Cisco ASA AIP-SSM-40 and Cisco IPS Sensor Software Version 6.1

General Information

Q. What is the Cisco® ASA AIP-SSM-40?

A. The Cisco ASA Advanced Inspection and Prevention Security Services Module 40 (AIP-SSM-40) is a hardware module that plugs into a Cisco ASA device and runs Cisco IPS Sensor Software, a comprehensive inline network-based defense system that is designed to accurately identify, classify, and stop malicious traffic, including worms, spyware, adware, and application abuse, before they affect your business or network assets.

Q. I already have a Cisco ASA appliance. Why do I need an AIP-SSM?

A. Cisco adaptive security appliances offer a combination of features, including firewall filtering, VPN termination, and inspection of Internet protocols such as HTTP and FTP. The Cisco ASA AIP-SSM extends Cisco intrusion prevention system (IPS) technology into SMB environments by combining high-performance inspection, reliability, and full firewall and IPS integration. With a Cisco ASA AIP-SSM solution, you can detect and prevent threats in all areas of your business network.

Q. What are the inspection and prevention capabilities of the Cisco ASA AIP-SSM-40?

A. The Cisco ASA AIP-SSM-40 uses the same advanced IPS capabilities available on all Cisco IPS sensors. Built on industry-leading Cisco security and network intelligence, the ASA AIP-SSM-40 runs Cisco IPS Sensor Software Version 6.0 or later, providing a comprehensive set of advanced inspections and signatures for known vulnerabilities, coupled with behavioral network anomaly detection for emerging “day-zero” threats.

Q. What is the performance of the Cisco ASA AIP-SSM-40 in my environment?

A. Cisco calculates the performance numbers for the Cisco ASA AIP-SSM-40 using a combination of the two most common Internet traffic profiles: media-rich and transactional traffic.

- **Media-rich traffic**

Media-rich environments are characterized by content. Web content seen on most popular Websites are media-rich, as are video content and file transfers.

- **Transactional traffic**

Transactional environments are characterized by shorter, more numerous connections. These include many types of e-commerce transactions, as well as instant messaging, voice, and lightweight interfaces such as RSS.

Also included in the performance calculation is the specific Cisco ASA appliance the AIP-SSM-40 has been installed in. The appliance throughput values are shown in the following table.

Cisco ASA Appliance Model	Firewall	Concurrent Threat Mitigation
Cisco ASA 5520 with AIP-SSM-40	450 Mbps	450 Mbps
Cisco ASA 5540 with AIP-SSM-40	650 Mbps	650 Mbps

Q. What configurations are available for the Cisco ASA AIP-SSM-40?

A. The Cisco ASA AIP-SSM-40 is available in two base configurations: installed in the Cisco ASA 5520 or 5540 Adaptive Security Appliance.

Q. How does the Cisco ASA AIP-SSM plug into and communicate with the appliance?

A. The Cisco ASA AIP-SSM plugs directly into the SSM slot in the Cisco ASA appliance's chassis. This provides a direct connection to the appliance's backplane. Once the module is installed, a proprietary protocol runs over the bus and controls data flow and messaging between the module and appliance.

Q. How does a user communicate with the Cisco ASA AIP-SSM-40?

A. The Cisco ASA AIP-SSM-40 has an external interface that needs to be plugged into the appropriate part of the network, based on the IP addressing information that was assigned to the Cisco IPS Sensor Software on the module. While configuration can be done using Cisco Adaptive Security Device Manager (ASDM), behind the scenes, Cisco ASDM is actually connecting to the module's address to perform configuration activities.

Q. For several years, Cisco has recommended a “defense-in-depth” approach, in which the firewall filters evaluate traffic before it is passed on to the IPS device for further inspection. Since I have IPS and firewall in the same device, how can I ensure that traffic is inspected for threats in the correct sequence?

A. Using the Cisco ASA AIP-SSM solution, all firewall filtering features happen before IPS inspection. Essentially, the recommendation described above is in place by default using this solution.

Q. If I'm using encrypted tunnels terminating on a Cisco ASA device, can I inspect the encrypted data using the AIP-SSM-40?

A. Yes. When the AIP-SSM-40 is installed in the Cisco ASA appliance, encrypted tunnels are terminated and then data is decrypted before being passed through the appliance device. This helps ensure that data that was encrypted is inspected before being routed out a Cisco ASA interface to its final destination.

Device Management**Q. How is the Cisco ASA AIP-SSM-40 managed?**

A. The Cisco ASA AIP-SSM-40 is managed by Cisco IPS Manager Express, a new IPS management software tool that is part of Cisco IPS Software Version 6.1. Cisco IPS Manager Express allows full management of IPS devices as well as advanced IPS alert reporting and sensor health management.

Q. How difficult is it to install and configure the Cisco ASA AIP-SSM-40?

A. The installation is an intuitive, six-step process.

1. Plug the AIP-SSM-40 card into your Cisco ASA 5520 or 5540 appliance.
2. Connect the management IP interface from the AIP-SSM-40 to your network.
3. Session into the AIP-SSM-40 from the appliance.
4. Run Setup and answer the prompts from the IPS setup wizard.
5. Launch Cisco ASDM and install the license and current IPS signatures list.
6. Create a security policy on the appliance, defining the traffic you would like to have inspected and in which manner (IDS or IPS).

Q. Does the Cisco ASA AIP-SSM-40 contain a hard drive? What is the expected mean time between failures?

A. In keeping with the resiliency requirements of the Cisco IPS 4200 Series, the Cisco ASA AIP-SSM-40 does not use a hard drive. This ensures that there are no moving parts in the module that would subject it to physical wear and tear and eventual hardware failure.

Cisco Services and Support

Q. How do I receive signature updates and support for the Cisco ASA AIP-SSM-40?

A. Cisco IPS devices require coverage of the module with “Cisco Services for IPS” to gain access to and install the latest signature updates for optimum security. “Cisco Services for IPS” provides continuously updated protection from external threats with regular signature, engine, and software updates. Cisco Services for IPS also protects your IPS investment with hardware maintenance support and access to the Cisco Technical Assistance Center (TAC), and keeps you abreast of the emerging threat landscape with a subscription to the Cisco IntelliShield Search Access Feature.

Q. Do I need both SMARTnet and Cisco Services for IPS to receive comprehensive support and signature updates?

A. No. “Cisco Services for IPS” is a support program for all Cisco solutions featuring Intrusion Prevention functionality. It combines features of SMARTnet support with IPS signature updates creating a comprehensive support program.

Please contact your account manager or reseller for more information on “Cisco Services for IPS.” To activate your subscription, please visit <http://www.cisco.com/go/license> .

Q. How do I access signature updates?

A. Customers with a “Cisco Services for IPS” contract can download signature updates using Cisco Security Manager or Cisco IPS Device Manager, or directly from <http://www.cisco.com/kobayashi/sw-center/ciscosecure/ids/crypto/index.shtml> .

Please note the serial number of the Cisco ASA AIP-SSM-40 must be covered by an active Cisco Services for IPS contract in order to install signature updates with any of above-mentioned methods.

Q. A Cisco ASA appliance is licensed according to the number of users and feature sets. How does this licensing scheme affect the Cisco ASA AIP-SSM-40?

A. This does not affect licensing for the Cisco ASA AIP-SSM-40. The module has no built-in intelligence to determine or enforce a concurrent number of users. The only license required on the module is “Cisco Services for IPS”, which is required to obtain IPS signature updates and IPS software updates.

Q. A Cisco ASA appliance is licensed according to the number of users and feature sets. What licensed feature set is required to run an AIP-SSM-40 card on the Cisco ASA appliance?

A. The Cisco ASA appliance does not require a license to run the Cisco ASA AIP-SSM-40.

Deployment

Q. Can the Cisco ASA AIP-SSM-40 protect my remote locations that need to access critical servers and data located at company headquarters?

A. Yes. The Cisco ASA AIP-SSM-40 solution runs the full suite of Cisco ASA firewall features and Cisco IPS features. This combination provides comprehensive security that can be deployed in any part of your network as long as the bandwidth of the module is not exceeded.

Q. Can the Cisco ASA AIP-SSM-40 protect my remote or local wireless networks?

A. Yes. Along with providing complete security features, the Cisco ASA AIP-SSM-40 solution also integrates into Cisco wireless controllers by accepting shun commands to stop malicious traffic on your wireless controllers, preventing the dangerous traffic from ever touching your main network.

Q. I currently run my Cisco ASA appliance in failover mode. Will the Cisco ASA AIP-SSM-40 solution work effectively in this deployment scenario?

A. Yes. The failover features of your Cisco ASA appliance will control which device is active. These features will maintain state in a failover condition, and will ensure unimpeded traffic flow if an appliance fails.

Q. I only want the Cisco ASA AIP-SSM-40 to inspect HTTP traffic, but my Cisco ASA appliance will be passing other traffic such as streaming video and telephony. Can I configure my module to only inspect HTTP traffic?

A. The traffic that is inspected by your Cisco ASA AIP-SSM-40 is fully user-definable from your Cisco ASA appliance. You may choose to inspect all traffic or a very specific subset—down to IP address and port information if desired.

Q. Can the Cisco ASA AIP-SSM-40 protect my IP telephony infrastructure, such as my Cisco Unified CallManager server?

A. The Cisco ASA AIP-SSM-40 solution is ideal for protecting protocols and data streams that are used for IP telephony, and for protecting the operating system and applications on a Cisco Unified CallManager server. Cisco IPS features include specific signatures for protecting IP telephony call setup, preventing Layer 2 man in the middle attacks, and stopping malicious code that can infect or exploit the Cisco Unified CallManager Server.

New Features in Cisco IPS Sensor Software 6.1

Q. What are the new features of Cisco IPS Sensor Software Version 6.1?

A. The new features of Cisco IPS Sensor Software Version 6.1 include a completely redesigned management interface. The smaller-scale event monitoring package, Cisco IPS Event Viewer, has been replaced by Cisco IPS Manager Express, which has been designed to better reflect user requirements.

Cisco IPS Manager Express is an installed application that integrates management of the IPS sensor along with monitoring. It includes:

- Completely redesigned reporting and health monitoring
- Redesigned sensor management for better usability and enhanced workflow
- Setup wizards to get a new user up and running in minimal time
- A policy table to give users a single place to view policy across their sensor
- The ability for the sensors to auto-updates directly from Cisco.com

- Q.** I get an error in Cisco IPS Manager Express when I try to view the configuration of one of my sensors running Cisco IPS Sensor Software Version 6.0.3E1. Is this expected behavior?
- A.** While Cisco IPS Manager Express can import and display events from a sensor running Cisco IPS Sensor Software Version 6.0.x, it cannot configure the events inside the application. You will need to launch the Cisco IPS Device Manager by opening a browser and HTTPS to the address of the sensor directly. In the case of the Cisco ASA AIP-SSM, this address is the module's management address, not the Cisco ASA appliance chassis itself.



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, CCVP, Cisco, Cisco StadiumField, the Cisco logo, CPE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play and Learn is a service mark; and Access Registrar, Altran, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSF, 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browser, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS IPbase, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuickStudy, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MIM, 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. ©2007