

## Cisco Intrusion Protection System Advanced Integration Module

### General

**Q. What is the Cisco® Intrusion Protection System Advanced Integration Module (IPS AIM)?**

**A.** The Cisco IPS AIM for the Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers is part of the Cisco IPS Sensor portfolio. It provides dedicated CPU and memory to offload inline and promiscuous intrusion protection processing. The AIM runs the Cisco IPS 6.0 sensor image to provide feature parity with Cisco IPS 4200 Series Sensors and Cisco ASA 5500 Series Adaptive Security Appliances.

**Q. Why do I need intrusion prevention at the branch if it is already being implemented at my company headquarters?**

**A.** With the movement toward any-to-any communications topologies for corporate WANs, not all traffic must traverse the data center when going from branch to branch. Also, branch offices are vulnerable for the introduction of worms and viruses. With IPS implemented at a branch office, attacks are identified and resolved at the edge of the network, before they can spread throughout the enterprise. A worm that spreads through the internal network before getting to the core IPS can cause a denial of service (DoS) on the core IPS.

**Q. When do I deploy Cisco IOS® IPS and when should I use the Cisco IPS AIM? Can they be used together?**

**A.** Cisco IOS IPS and the Cisco IPS AIM cannot be used together. Cisco IOS IPS must be disabled when the AIM IPS is installed. Cisco IOS IPS is an IPS application that provides inspection capabilities for traffic flowing through the router. Although it is included in the Cisco IOS Advanced Security feature set, it uses the router CPU and shared memory pool to perform the inspection. Cisco IOS IPS also runs a subset of IPS signatures. The Cisco AIM IPS runs with a dedicated CPU and memory, offloading all processing of IPS signatures from the router CPU. It can load a full signature set and provide enhanced IPS features not available on Cisco IOS IPS.

**Q. What are the most typical deployment scenarios for the Cisco IPS AIM?**

**A.** The most common deployment scenarios are to protect the WAN link and corporate offices and to protect servers at remote sites. Whether a private or public connection, the WAN link is vulnerable to threats introduced at the branch office. With IPS implemented at the branch, attacks can be mitigated at the WAN edge before they propagate to other parts of the network. Similarly, servers at remote sites often contain data as valuable as those at the corporate data center. Isolating threats before they attack these servers protects that data from compromise. Finally, commercial and small to medium-sized businesses (SMBs) can benefit from the Cisco IPS AIM in their Internet routers to add protection to their main network.

**Q. What type of branch office is best suited to take advantage of IPS?**

**A.** Virtually any branch office can benefit from IPS. Branches most at risk are those with no corporate IT staff, where the branch or store manager focuses on running the business rather than enforcing corporate IT policies.

**Q. What is the part number of the Cisco IPS AIM?**

**A.** The part number of the Cisco IPS AIM is AIM-IPS-K9.

**Q. What platforms support the Cisco IPS AIM?**

**A.** It is supported on the Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers. Although it is an AIM, it is not supported in older platforms with AIM slots, such as the Cisco 2600 and 3700 Series Multiservice Access Routers. Installation in these platforms may cause irreversible damage to the card and the platform.

**Q. What feature sets support the Cisco IPS AIM?**

**A.** It is supported in the Cisco IOS Advanced Security feature set and above, including the Cisco IOS Advanced IP Services and Advanced Enterprise Services feature sets.

**Q. What is the meaning of K9 in the product part number?**

**A.** K9 is the designator of strong encryption, including Triple Digital Encryption Standard (3DES) and Advanced Encryption Standard (AES). Even though the Cisco IPS AIM is supported in nonsecurity images such as IPBASE, the card is designated as a K9 product because the card itself includes strong encryption in the Secure Shell (SSH) Protocol. The K9 designation allows Cisco to control shipment of cryptography-enabled devices and software and comply with U. S. State Department rules on the export of such devices.

**Q. What Cisco IOS Software releases support Cisco IPS AIM?**

**A.** Cisco IPS AIM is supported on Cisco IOS Software Releases 12.4(15) XY and 12.5(1st)T.

**Q. Does the Cisco IPS AIM support IPv6?**

**A.** No. The Cisco IPS AIM and NM currently does not support IPv6.

**Q. Does the Cisco IPS AIM monitor multicast traffic?**

**A.** No. The Cisco IPS AIM does not monitor multicast traffic.

**Q. What are the differences between the Cisco IPS AIM and Cisco IOS IPS?**

**A.** Following are some of the major differences between the Cisco IPS AIM and Cisco IOS IPS:

- Cisco IPS AIM has dedicated CPU and DRAM to offload IPS processing, whereas Cisco IOS IPS shares router resources with other processes.
- Cisco IPS AIM supports both inline and promiscuous mode, whereas Cisco IOS IPS supports only inline mode.
- Cisco IPS AIM supports the full IPS signature set, whereas Cisco IOS IPS supports a subset.
- Cisco IPS AIM runs a Linux-based Cisco IPS 6.0 sensor image, whereas Cisco IOS IPS runs a Cisco IOS Software-based IPS code.

**Q. What are the differences between the Cisco IPS AIM and the Cisco Intrusion Detection System (IDS) Network Module?**

**A.** Following is a list of major differences between the Cisco IPS AIM and the Cisco IDS Network Module:

- Cisco IPS AIM supports both inline and promiscuous mode, whereas the Cisco IDS Network Module supports only promiscuous mode.
- Cisco IPS AIM is managed internally through the router ports, whereas the Cisco IDS Network Module is managed through the external management port on the card.
- Cisco IPS AIM has 256-MB EUSB flash memory, whereas the Cisco IDS Network Module has a 40-GB hard disk.

## Installation and Configuration

### Q. How do I access the console of the Cisco IPS AIM?

**A.** The Cisco IPS AIM is accessed by using the **service-module ids-sensor 0/0 session** command, which initiates a reverse Telnet session and effectively puts the user at the console prompt of the AIM. From this point, configuration is performed in the Cisco IDS application and not in Cisco IOS Software. To exit the AIM, use the CTRL+ALT+^ key sequence, which closes the reverse Telnet session and leaves the user at the Cisco IOS command prompt.

### Q. How is the Cisco IPS AIM numbered?

**A.** The Cisco IOS IDS-Sensor interface uses the slot or port numbering scheme. For the Cisco IPS AIM, the slot number is always 0 and the port number is the AIM slot number. An IPS AIM in AIM slot 0 is IDS-Sensor0/0, and an IPS AIM in AIM slot 1 is IDS-Sensor 0/1.

### Q. What are boot loader and minikernel?

**A.** A boot loader is software that locates and loads an operating system and jumps to it. The Cisco IPS AIM has two boot loaders: runtime boot loader and failsafe boot loader. The runtime boot loader is executed in normal operation. If the runtime boot loader fails, the card falls back to failsafe boot loader. The runtime boot loader can be upgraded, but the failsafe boot loader cannot.

A minikernel is used to read an IPS sensor image indicated by the boot loader configuration file off the USB flash device and execute the image with the specified parameters. The minikernel is called automatically by the runtime boot loader when the card is configured to be in normal mode.

### Q. Where do I find the latest IPS sensor image for the Cisco IPS AIM?

**A.** IPS software can be accessed at <http://www.cisco.com/kobayashi/sw-center/ciscosecure/ids/crypto/>

### Q. How do I upgrade IPS sensor image?

**A.** Instructions for upgrading the application are at [http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_installation_guides_list.html)

### Q. How do I set the IPS sensor in bypass mode?

**A.** To set the IPS sensor in bypass mode, perform the following steps:

- Session into the sensor.
- From the sensor prompt, enter the **configure terminal** command.
- From the sensor config prompt, enter the **service interface** command.
- From the sensor config-int prompt, enter the **bypass off|on|auto** command. The Off option turns off inline bypassing. Packet inspection is performed on inline data traffic. However, inline traffic is interrupted if the IPS analysis engine is stopped. The On option turns on inline bypassing. No packet inspection is performed on the traffic. Inline traffic continues to flow even if the analysis engine is stopped. The Auto option automatically begins bypassing

inline packet inspection if the analysis engine stops processing packets. This option prevents data interruption on inline interfaces.

**Q. If for some reason the Cisco IPS AIM cannot inspect the packets, will the traffic pass through or be dropped?**

**A.** If the Cisco IPS AIM cannot inspect a specific packet or all packets, the user can determine if the packet is dropped or passed on without inspection. This choice is made through the **service module fail-close** or **service-module fail-open** configuration command under the Cisco IOS IDS-Sensor interface.

```
atg2851-21#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
atg2851-21(config)#interface IDS-Sensor 0/0
atg2851-21(config-if)#service-module ?
    fail-close  Blocks traffic if Service Module fails
    fail-open   Permits traffic if Service Module fails
```

With fail-open, the traffic that cannot be inspected is sent without being inspected. With fail-close, the traffic that cannot be inspected is dropped. Fail-open is the default.

**Q. Can the IPS sensor image and Cisco IOS Software image be upgraded independently?**

**A.** Yes.

**Q. Do the Cisco IPS AIM and the Cisco IDS Network Module use the same image?**

**A.** No, they use different IPS sensor images.

**Q. I cannot configure the ids-service-module monitoring command under a Layer 2 Cisco EtherSwitch® interface. Why?**

**A.** The **ids-service-module monitoring** command is not allowed under a Layer 2 interface. Please assign the Layer 2 interface to a VLAN and configure the monitoring command under the VLAN.

### Integration and Interoperability

**Q. Can I request my service provider to manage IPS?**

**A.** Yes, your service provider may offer managed IPS service that can include installation, monitoring and maintenance of the IPS. Please check their SLA to understand what services SP is providing. For detailed information, please visit [www.cisco.com/go/securityservices](http://www.cisco.com/go/securityservices)

**Q. What should be my Service Level Agreement with SP for the Managed IPS service?**

**A.** Most of the security SLA revolve around response time during the security incident.



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](http://www.cisco.com/go/offices).

CCDF, CCENT, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks. Changing the Way We Work, Live, Play, and Learn is a service mark and Access Register. Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCBA, CDDP, CCSE, CCSP, CCNA, CCNP, CCSP, 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IQ Experience, the IQ logo, IQ Net, Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MEX, NetScout, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SNA First, 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. (080239)