Cisco Intrusion Prevention System Modules for the Cisco Integrated Services Routers

General

Q. What are the Cisco® Intrusion Prevention System (IPS) modules for the integrated services routers?

A. There are two IPS modules for the integrated services routers -- the Cisco Intrusion Prevention System Advanced Integration Module (IPS AIM) and the Intrusion Prevention System Network Module Enhanced (IPS NME). They are part of the Cisco IPS Sensor portfolio. Both modules provide dedicated CPU and memory to offload inline and promiscuous intrusion protection processing. The modules run the Cisco IPS Sensor Software to provide feature parity with Cisco IPS 4200 Series Sensors and Cisco ASA 5500 Series Adaptive Security Appliances. The Cisco IPS AIM is supported in the Cisco 1841 and Cisco 2800 and 3800 Series and the IPS NME is supported in the Cisco 2811, 2821, 2851, 2911, 2921, 2951 and Cisco 3800 and 3900 Series Integrated Services Routers.

Q. Why do I need intrusion prevention at the branch office 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 office to branch office. Also, branch offices are vulnerable to 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. What are the most typical deployment scenarios for the Cisco IPS modules?

A. The most common deployment scenarios are to protect the WAN link and corporate offices and to protect servers at remote sites. Whether it is a private or public connection, the WAN link is vulnerable to threats introduced at the branch office. With IPS implemented at the branch office, you can mitigate attacks at the WAN edge before they propagate to other parts of the network. Similarly, servers at remote sites often contain data as valuable as the data at servers at the corporate data center. Isolating threats before they attack these servers protects that data from compromise. Finally, commercial and small and 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. Branch offices most at risk are those with no corporate IT staff, where the branch-office or store manager focuses on running the business rather than enforcing corporate IT policies.

Q. What are the part numbers of the Cisco IPS AIM and IPS NME?

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

Q. What platforms support the Cisco IPS AIM?

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

Q. What platforms support the Cisco IPS NME?

A. The IPS NME slot is supported on the Cisco 2811, 2821, and 2851 and Cisco 3800 Series Routers. The IPS NMEis also supported with a jacket card on 2911, 2921, 2951 and Cisco 3900 Series Routers..

Q. What feature sets support the Cisco IPS modules?

A. On Cisco 1841, 2800 and 3800 Series Routers, the Cisco IOS® Advanced Security feature set, Advanced IP Services set and Advanced Enterprise Services feature set support those modules. However, 2911, 2921, 2951 and Cisco 3900 Series Routers do not require a Security Feature license to support IPS NME module.

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). The Cisco IPS AIM and IPS NME 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 modules?

A. Cisco IPS AIM is supported on Cisco IOS Software Releases 12.4(15) XY and 12.4(20)T or later. Cisco IPS NME is supported on Cisco IOS Software Release 12.4(20)YA and 12.4(22)T or later on 2800 and 3800 Series Routers. In addition, it is supported on 2900 and 3900 Series Routers starting with Cisco IOS 15.0(1)M Release.

Q. When do I deploy Cisco IOS IPS and when should I use the Cisco IPS module? Can I use them together?

A. Cisco IOS IPS is a Cisco IOS Software feature that provides IPS inspection capabilities for traffic flowing through the router. You cannot use Cisco IOS IPS and the Cisco IPS modules together. Cisco IOS IPS must be disabled when the IPS AIM or IPS NME is installed.

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

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

- Cisco IPS AIM and IPS NME have dedicated CPU and DRAM to offload IPS processing, whereas Cisco IOS IPS shares router resources with other processes.
- Cisco IPS AIM and IPS NME support both inline and promiscuous mode, whereas Cisco IOS IPS supports only inline mode.
- Cisco IPS AIM and IPS NME can support all Cisco IPS signatures that are not retired by default, whereas Cisco IOS IPS can support only a user configurable subset.
- Cisco IPS AIM and IPS NME run Linux-based Cisco IPS Sensor Software, 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 IPS NME?

A. The Cisco IPS AIM and IPS NME differ in the following ways:

- **Form factor:** The IPS NME is a different form factor from the IPS AIM and is externally accessible. You can insert the IPS NME into any of the available NME slots without removing the cover.
- **Performance:** The IPS AIM supports up to 45 Mbps, whereas the IPS NME runs up to 75 Mbps.
- **Module and card support for integrated services routers:** The IPS NME slot(s) is supported on Cisco 2811 and higher 2800 and 3800 Series models. The IPS NME module requires a jacket card to be installed on on Cisco 2911 and higher 2900 and 3900 Series models . The IPS AIM is supported on Cisco1841 and higher 2800 and 3800 Series models only.

- **Online insertion and removal (OIR):** OIR is supported with the IPS NME on the Cisco 3945 only; it is not supported with the IPS AIM. OIR is for replacement of like-to-like modules. Addition of a new module requires the platform to be rebooted.
- **Management port for the IPS AIM and IPS NME:** An external Ethernet management port is available on the IPS NME for all configuration, management, and monitoring of the module. The IPS AIM uses the internal interface for all network and management traffic. There is a difference between the numbering of the management interface for the IPS AIM (Management0/0) and that of the IPS NME (Management0/1). And when you issue a show interfaces command, the output identifies the IPS AIM with IDS-Sensor0/X, where the X indicates the AIM slot. The IPS NME is identified with IDS-SensorY/0, where the Y indicates the NME slot.
- **Cisco IPS Sensor Software version support:** The Cisco IPS NME supports Cisco IPS Sensor Software Version 6.1(1) and later. IPS AIM support began with Cisco IPS Sensor Software Version 6.0(4) and later. Both support Clobal Correlation based IPS solution in Cisco IPS Software 7.0 and later releases in line with those of Cisco IPS 4200 Series Sensors.

Installation and Configuration

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

A. You can access the Cisco IPS AIM by using the service-module ids-sensor 0/X session command, which initiates a reverse Telnet session and effectively puts you at the AIM console prompt. From this point, you configure in the Cisco IPS 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 you at the Cisco IOS Software command prompt. You can access the IPS NME by using the service-module ids-SensorY/0 session command, where the Y indicates the NME slot.

Q. How are the Cisco IPS modules 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. The IPS NME is identified with IDS-SensorY/0, where the Y indicates the NME slot.

Q. What are the boot loader and minikernel?

A. A boot loader is software that locates and loads an operating system. The CPU execution order is then interrupted to run the operating system code just loaded on the CPU program memory. 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 CPU 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 memory 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 run in normal mode.

Q. Where do I find the latest Cisco IPS Sensor Software image for the Cisco IPS modules?

A. You can access IPS software at http://www.cisco.com/kobayashi/sw-center/ciscosecure/ids/crypto/.

Q. How do I upgrade the IPS sensor image?

A. Instructions for upgrading the application are available at: http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_installation_guides_list.html.

Q. Can I install both the Cisco IPS AIM and IPS NME on the same integrated services router?

A. No. Only one IPS sensor module can be enabled on an integrated services router.

Q. If for some reason the Cisco IPS modules 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, you can determine if the packet is dropped or passed on without inspection. You can make this choice through the service module fail-close or service-module fail-open configuration command under the Cisco IOS IDS Sensor interface:

```
c2851#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
c2851(config)#interface IDS-Sensor 0/0
c2851(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. 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. Can I upgrade the Cisco IPS Sensor Software image and Cisco IOS Software image independently?

A. Yes.

Q. Do the Cisco IPS modules support IPv6?

A. No. The Cisco IPS AIM and IPS NME currently do not support IPv6.

Q. Do the IPS modules monitor multicast traffic?

A. No. The Cisco IPS modules do not monitor multicast traffic.

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.

Service and Support

Q. How do I order support and signature file updates for the Cisco IPS AIM and IPS NME?

A. Cisco Services for IPS is a technical support service designed to support products that feature IPS functions. It includes Cisco SMARTnet® support, which covers hardware replacement options; Cisco Technical Assistance Center (TAC) support; registered access to Cisco.com; operating-system updates; and subscription to signature updates to help ensure the IPS-enabled products detect, classify, control, and prevent intrusions in real time. Cisco Services for IPS also includes access to the Cisco IntelliShield Search Access feature for detailed research on the latest threats and vulnerabilities correlated with IPS signatures.

Cisco Services for IPS for Cisco IPS AIM or Cisco IPS NME includes Cisco SMARTnet support for the module but does not cover the Cisco SMARTnet support for the host platform. You must purchase Cisco SMARTnet support for the Cisco 1841 and Cisco 2800, 2900, 3800 and 3900 Series Routers separately. Also, the service level of the two Cisco SMARTnet service contracts must be the same. For example, if you wish to order the Cisco 2811 SEC bundle and Cisco IPS AIM with a service level of 8x5 next business day (NBD), you need two service contracts: their part numbers are CON-SNT-2811SEC (Cisco SMARTnet support with Advanced Replacement parts delivery 8x5 Next Business Day for the Cisco 2811 with Security bundle) and CON-SU1-AIMIPSK9 (Cisco Services for IPS contract that includes both Cisco SMARTnet support with Advanced Replacement parts delivery 8x5 Next Business Day for AIM-IPS-K9 module and subscription license for Cisco IPS signature updates for AIM-IPS-K9 module).

Note: You cannot purchase the signature subscription by itself; you must also purchase Cisco Services for IPS support .

More information, including a step-by-step guide, is available at: http://www.cisco.com/en/US/products/ps6076/serv_group_home.html.

Q. Can I ask 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 your provider's service-level agreement (SLA) to understand what services it provides. For detailed information, please visit http://www.cisco.com/go/securityservices.

Q. What should be my SLA with my service provider for the managed IPS service?

A. Most of the security SLAs 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.

Printed in USA C67-423800-04 08/09