Configuring the AIM IPS

> **Note** All IPS platforms allow ten concurrent log in sessions.

This chapter describes how to configure the AIM IPS and get it ready to receive IPS traffic. After that you are ready to configure intrusion prevention. It contains the following sections:

AIM IPS Configuration Sequence

Perform the following tasks to configure the AIM IPS:

1. Set up the interfaces.
2. Log in to the AIM IPS.
3. Initialize the AIM IPS.

   Run the **setup** command to initialize the AIM IPS.
4. Create the service account.

> ⚠ **Caution** You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a new password if the administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

5. Perform the other initial tasks, such as adding users, trusted hosts, and so forth.

6. Configure intrusion prevention.

7. Perform administrative tasks to keep your AIM IPS running smoothly.

8. Upgrade the IPS software with new signature updates and service packs.

9. Reimage the boot helper and bootloader when needed.

For More Information

- For the procedure for setting up interfaces, see Setting Up Interfaces on the AIM IPS and the Router, page 17-4.

- For the procedure for logging in to the AIM IPS, see Establishing Sessions, page 17-13.

- For the procedure for running the **setup** command on the AIM IPS, see Advanced Setup for the AIM IPS, page 3-12.

- For the procedure for creating the service account, see Creating the Service Account, page 4-14.

- For the procedures for setting up the sensor, see Chapter 4, "Setting Up the Sensor."

- For the procedures for configuring intrusion prevention, see Chapter 9, "Configuring Anomaly Detection," Chapter 7, "Configuring Event Action Rules," Chapter 8, "Defining Signatures," and Chapter 13, "Configuring Attack Response Controller for Blocking and Rate Limiting."

- For the procedures to keep your sensor running smoothly, see Chapter 16, "Administrative Tasks for the Sensor."

- For more information on obtaining Cisco IPS software, see Obtaining Cisco IPS Software, page 21-1.

- For the procedure for reimaging the AIM IPS, see Installing the AIM IPS System Image, page 22-21.

Verifying Installation and Finding the Serial Number

Use the **show inventory** command in privileged EXEC mode to verify the installation of the AIM IPS.

Note You can also use this command to find the serial number of your AIM IPS for use in troubleshooting with TAC. The serial number appears in the PID line, for example, SN: FOC11372M9X.

To verify the installation of the AIM IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Verify that the AIM IPS is part of the router inventory.

```
router# show inventory
NAME: "3825 chassis", DESCR: "3825 chassis"
PID: CISCO3825 , VID: V01 , SN: FTX1009C3KT
```

```
NAME: "Cisco Intrusion Prevention System AIM in AIM slot: 1", DESCR: "Cisco Intrusion
Prevention"
PID: AIM-IPS-K9 , VID: V01 , SN: FOC11372M9X

router#
```
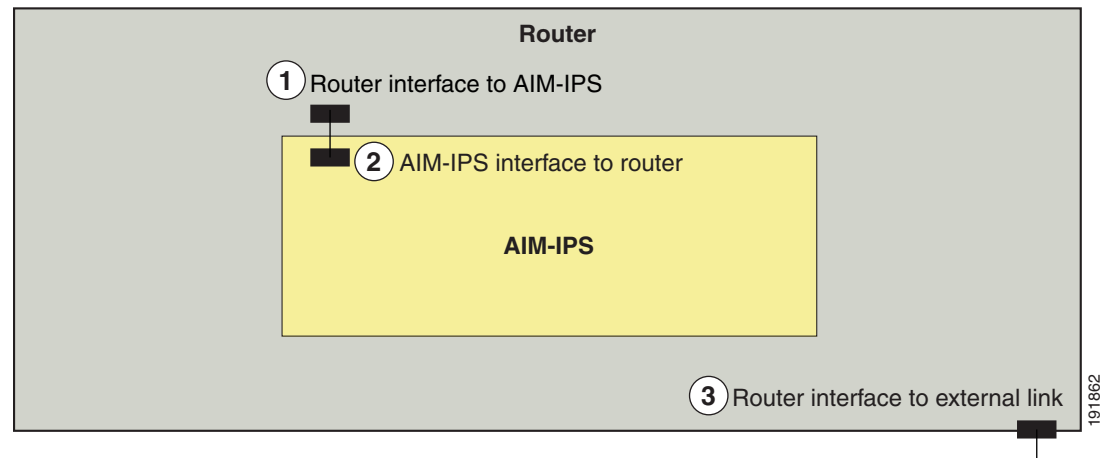
Understanding the Hardware Interfaces

Figure 17-1 shows the router and AIM IPS interfaces used for internal communication. You can configure the router interfaces through the Cisco IOS CLI and the AIM IPS interfaces through the IPS CLI, IDM, IME, or CSM.

Figure 17-1   AIM IPS and Router Interfaces

1	Router interface to the AIM IPS (IDS-Sensor 0/1) Uses the Cisco OS CLI to configure the IP address of the router interface that connects to the AIM IPS. This router IP address is used as the default router IP address when you configure Cisco IPS on the AIM IPS.
2	The AIM IPS interface to router (GigabitEthernet0/1) Configure the command and control interface using the IPS CLI, IDM, IME, or CSM.
3	Router interface to external link.

Note   You need two IP addresses to configure the AIM IPS. The AIM IPS has a command and control IP address that you configure through the Cisco IPS CLI. You also assign an IP address to the router for its internal interface (IDS-Sensor 0/x) to the AIM IPS. This IP address belongs to the router itself and is used for routing traffic to the command and control interface of the AIM IPS. It is used as the default router IP address when you set up the AIM IPS command and control interface.

Setting Up Interfaces on the AIM IPS and the Router

This section describes how to set up interfaces on the AIM IPS and the router, and contains the following topics:

Interface Configuration Sequence

Follow this sequence to set up interfaces on the AIM IPS and the router:

1. Configure the IPS command and control interface on the router, and the AIM IPS IP address, mask, and gateway using one of the following methods:

    - An unnumbered IP address on the IDS-Sensor interface

        ✎
        Note Using an unnumbered IP address on the IDS-Sensor interface is the preferred method for configuring interfaces on the module and router.

    - A routable IP address
    - Default module IP address with NAT
    - User-configured IP address with NAT

2. Enable the monitoring interface and specify whether it is promiscuous or inline, assign the ACL to the interface, specify how you want the router to handle traffic if the module fails, and create a monitoring ACL (optional).

3. Save the configuration.

For More Information

- For the procedure for configuring an unnumbered IP address on the IDS-Sensor interface, see Using an Unnumbered IP Address Interface, page 17-5.
- For the procedure for configuring a routable IP address, see Using a Routable IP Address Interface, page 17-7.
- For the procedure for configuring the default module IP address using NAT, see Using a Default IP Address and NAT, page 17-9.
- For the procedure for configuring the IP address with NAT, see Using a User-Configured IP Address and NAT, page 17-10.
- For the procedure for enabling the monitoring interface, see Configuring Monitoring on the Router Interface, page 17-12.

ARC and NAT

If you use NAT to establish management access to the AIM IPS, ARC on the AIM IPS does not know the external IP address of the AIM IPS. To make sure that management access to the AIM IPS is not interrupted by devices that the AIM IPS is managing, you must state the NAT address of the AIM IPS every time you add a blocking device.

For More Information

- For more information on ARC, see Chapter 13, "Configuring Attack Response Controller for Blocking and Rate Limiting."

- For the procedures for configuring the AIM IPS NAT address every time you add a blocking device, see the following procedures:

  - Configuring the Sensor to Manage Cisco Routers, page 13-22
  - Configuring the Sensor to Manage Catalyst 6500 Series Switches and Cisco 7600 Series Routers, page 13-25
  - Configuring the Sensor to Manage Cisco Firewalls, page 13-27

Using an Unnumbered IP Address Interface

> **Note**   Using an unnumbered IP address on the IDS-Sensor interface is the preferred method for configuring interfaces on the AIM IPS and the router.

To configure the interface using an unnumbered IP address interface, follow these steps:

Step 1   Log in to the router.

Step 2   Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3   Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor0/1
router#
```

Step 4   Configure the IPS command and control interface on the router using the **ip unnumbered** command on the IDS-Sensor interface to specify the router interface that provides external connectivity:

a.   Make sure the IDS-Sensor interface is not shut down.

```
router# configure terminal
router(config)# interface ids-sensor 0/1
router(config-if)# no shutdown
```

b.   Specify the external router interface.

```
router(config-if)# ip unnumbered other_router_interface
router(config-if)# exit
router(config)#
```

> **Note** The IDS-Sensor interface shares the IP address between the two router interfaces (the
> IDS-Sensor interface and the other specified interface).

> **Note** The IP address of the sensor and the *other_router_interface* IP address must be on the same
> subnet.

c. Enter a route to send traffic to the IP address of the AIM IPS to the IDS-Sensor interface.

```
router(config)# ip route sensor_ip_address 255.255.255.255 ids-sensor 0/1
router(config)#
```

d. Exit configuration mode.

```
router(config)# exit
router#
```

Step 5 Configure the IP address, mask, and gateway:

> **Note** You can also configure these parameters by initializing the AIM IPS with the **setup** command.

> **Note** The AIM IPS IP address defaults to 192.168.1.2/24,192.168.1.1.

a. Session to the AIM IPS.

```
router# service-module ids-sensor 0/1 session
Trying 192.168.1.2, 2322 ... Open


sensor login:
```

b. Log in to the CLI.

c. Enter global configuration mode.

```
sensor# configure terminal
sensor(config)#
```

d. Enter service host mode.

```
sensor(config)# service host
sensor(config-hos)#
```

e. Assign the command and control interface and the gateway.

```
sensor(config-hos)# network-settings
sensor(config-hos-net)# host-ip ip_address/mask,gateway
sensor(config-hos-net)#
```

> **Note** The gateway should be the IP address of the *other_router_interface* that you set up in
> Step 4b.

f. Exit network settings mode.

```
sensor(config-hos-net)# exit
```

```
sensor(config-hos)# exit
Apply Changes:?[yes]:
```

g. Press **Enter** to apply the changes or enter **no** to discard them.

h. Exit the session to the AIM IPS.

Step 6   Write the configuration to NVRAM.

```
router# write memory
Building configuration
[OK]
```

For More Information

- For the procedure for using the **setup** command to initialize the AIM IPS, see Advanced Setup for the AIM IPS, page 3-12.

- For more information on sessioning from the router to the AIM IPS and exiting sessions, see Opening and Closing a Session, page 17-14.

Using a Routable IP Address Interface

To configure the interface using a routable IP address interface, follow these steps:

Step 1   Log in to the router.

Step 2   Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3   Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor0/1
router#
```

Step 4   Configure the IPS command and control interface on the router using the **ip unnumbered** command on the IDS-Sensor interface to specify the router interface that provides external connectivity:

a. Make sure the IDS-Sensor interface is not shut down.

```
router# configure terminal
router(config)# interface ids-sensor 0/1
router(config-if)# no shutdown
```

b. Configure an IP address for the IDS-Sensor interface.

```
router(config-if)# ip address 192.168.1.2 255.255.255.0
router(config0if)#
```

Use 192.168.1.2 (default IP address for the default gateway on the AIM IPS). You cannot session to the AIM IPS if its interface does not have an IP address.

c. Enter a route to send traffic to the IP address of the AIM IPS to the IDS-Sensor interface.

```
router(config)# ip route sensor_ip_address 255.255.255.255 ids-sensor 0/1
router(config)#
```

d. Exit configuration mode.

```
router(config)# exit
router#
```

Step 5   Configure the AIM IPS IP address, mask, and gateway:

✎

Note   The AIM IPS IP address defaults to 192.168.1.2/24,192.168.1.1.

a. Session to the AIM IPS.

```
router# service-module ids-sensor 0/1 session
Trying 192.168.1.2, 2322 ... Open


sensor login:
```

b. Log in to the CLI.

c. Enter global configuration mode.

```
sensor# configure terminal
sensor(config)#
```

d. Enter service host mode.

```
sensor(config)# service host
sensor(config-hos)#
```

e. Assign the command and control interface and the gateway.

```
sensor(config-hos)# network-settings
sensor(config-hos-net)# host-ip ip_address/mask,gateway
sensor(config-hos-net)#
```

f. Exit network settings mode:

```
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes:?[yes]:
```

g. Press **Enter** to apply the changes or enter **no** to discard them.

h. Exit the session to the AIM IPS.

Step 6   Write the configuration to NVRAM.

```
router# write memory
Building configuration
[OK]
```

For More Information

- For the procedure for using the **setup** command to initialize the AIM IPS, see Advanced Setup for the AIM IPS, page 3-12.

- For more information on sessioning from the router to the AIM IPS and exiting sessions, see Opening and Closing a Session, page 17-14.

Using a Default IP Address and NAT

To configure the interfaces using the default IP address and NAT, follow these steps:

Step 1   Log in to the router.

Step 2   Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3   Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor0/1
router#
```

Step 4   Configure the IPS command and control interface on the router using the default sensor IP address and have the router perform NAT:

a.   Make sure the IDS-Sensor interface is not shut down.

```
router# configure terminal
router(config)# interface ids-sensor 0/1
router(config-if)# no shutdown
```

b.   Configure an IP address for the IDS-Sensor interface (should match the default gateway that is configured on the AIM IPS).

```
router(config-if)# ip address 192.168.1.2 255.255.255.0
router(config0if)#
```

Use 192.168.1.2 (default IP address for the default gateway on the AIM IPS). You cannot session to the AIM IPS if its interface does not have an IP address.

c.   Set up a NAT address for the AIM IPS (the AIM IPS default IP address is 192.168.1.2).

```
router(config-if)# ip nat inside
router(config-if)# exit
router(config)# interface router_nat_outside_interface
router(config-if)# ip nat outside
router(config-if)# exit
router(config)# ip nat inside source static 192.168.1.2 aim_external_ip_address
router(config-if)# exit
```

> ✎
>
> **Note**   The *aim_external_ip_address* and the *router_nat_outside_interface* IP addresses must be on the same subnet. The IP address of the AIM IPS must be on a separate subnet.

d.   Exit configuration mode.

```
router(config-if)# exit
router(config)# exit
router#
```

Step 5   Configure the AIM IPS IP address, mask, and gateway:

> ✎
>
> **Note**   The AIM IPS IP address defaults to 192.168.1.2/24,192.168.1.1.

a.   Session to the AIM IPS.

```
router# service-module ids-sensor 0/1 session
Trying 192.168.1.2, 2322 ... Open


sensor login:
```

b. Log in to the CLI.

c. Enter global configuration mode.

```
sensor# configure terminal
sensor(config)#
```

d. Enter service host mode.

```
sensor(config)# service host
sensor(config-hos)#
```

e. Assign the command and control interface and the gateway.

```
sensor(config-hos)# network-settings
sensor(config-hos-net)# host-ip ip_address/mask,gateway
sensor(config-hos-net)#
```

f. Exit network settings mode.

```
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes:?[yes]:
```

g. Press **Enter** to apply the changes or enter **no** to discard them.

h. Exit the session to the AIM IPS.

Step 6   Write the configuration to NVRAM.

```
router# write memory
Building configuration
[OK]
```

For More Information

- For the procedure for using the **setup** command to initialize the AIM IPS, see Advanced Setup for the AIM IPS, page 3-12.

- For more information on sessioning from the router to the AIM IPS and exiting sessions, see Opening and Closing a Session, page 17-14.

- For more information on how ARC and NAT operate on the AIM IPS, see ARC and NAT, page 17-5.

Using a User-Configured IP Address and NAT

To configure the interfaces using a user-configured IP address and NAT, follow these steps:

Step 1   Log in to the router.

Step 2   Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3   Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor0/1
router#
```

Step 4   Configure the IPS command and control interface on the router using the default sensor IP address and have the router perform NAT:

a.   Make sure the IDS-Sensor interface is not shut down.

```
router# configure terminal
router(config)# interface ids-sensor 0/1
router(config-if)# no shutdown
```

b.   Configure an IP address for the IDS-Sensor interface.

```
router(config-if)# ip address user_configured_ip_address gateway
router(config0if)#
```

You cannot session to the AIM IPS if its interface does not have an IP address.

c.   Set up a NAT address for the AIM IPS.

```
router(config-if)# ip nat inside
router(config-if)# exit
router(config)# interface router_nat_outside_interface
router(config-if)# ip nat outside
router(config-if)# exit
router(config)# ip nat inside source static AIM_ip_address AIM_external_ip_address
router(config-if)# exit
```

d.   Exit configuration mode.

```
router(config-if)# exit
router(config)# exit
router#
```

Step 5   Configure the AIM IPS IP address, mask, and gateway:

> **Note**   The AIM IPS IP address defaults to 192.168.1.2/24,192.168.1.1.

a.   Session to the AIM IPS.

```
router# service-module ids-sensor 0/1 session
Trying 192.168.1.2, 2322 ... Open


sensor login:
```

b.   Log in to the CLI.

c.   Enter global configuration mode.

```
sensor# configure terminal
sensor(config)#
```

d.   Enter service host mode.

```
sensor(config)# service host
sensor(config-hos)#
```

e.   Assign the command and control interface and the gateway.

```
sensor(config-hos)# network-settings
```

```
sensor(config-hos-net)# host-ip ip_address/mask,gateway
sensor(config-hos-net)#
```

f. Exit network settings mode.

```
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes:?[yes]:
```

g. Press **Enter** to apply the changes or enter **no** to discard them.

h. Exit the session to the router.

Step 6   Write the configuration to NVRAM.

```
router# write memory
Building configuration
[OK]
```

For More Information

- For the procedure for using the **setup** command to initialize the AIM IPS, see Advanced Setup for the AIM IPS, page 3-12.

- For more information on sessioning from the router to the AIM IPS and exiting sessions, see Opening and Closing a Session, page 17-14.

- For more information on how ARC and NAT operate on the AIM IPS, see ARC and NAT, page 17-5.

Configuring Monitoring on the Router Interface

Note   You must add the AIM IPS internal interface to the virtual sensor (vs0) so that traffic can be monitored.

To configure the router interface to be monitored, follow these steps:

Step 1   Log in to the router.

Step 2   Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3   (Optional) Configure a monitoring access list on the router.

```
router(config)# access-list 101 permit tcp any eq www any
```

You can set up a standard access list and apply it to filter what type of traffic you want to inspect. A matched ACL causes traffic not to be inspected for that ACL. This example bypasses inspection of HTTP traffic only. Refer to your Cisco IOS Command Reference for more information on the options for the **access-list** command.

Step 4   Enable monitoring on the interface in either inline or promiscuous mode and associate the access list.

```
router(config)# interface monitored_interface
router(config-if)# ids-service-module monitoring [inline | promiscuous] access-list 101
router(config-if)# exit
router(config)#
```

> **Note**   Associating the access list with the interface further controls what traffic is sent to the AIM IPS.

Step 5   (For inline mode) Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor0/1
router#
```

Step 6   (For inline mode) Specify how the router handles traffic inspection during a module failure.

```
router(config)# interface ids-sensor 0/1
router(config-if)# service-module [fail-close | fail-open]
router(config-if)#
```

The default is fail-open.

> **Note**   The **fail-close** option means that if the AIM IPS fails, then the router does not let traffic pass. The **fail-open** option means if the AIM IPS fails, the router lets traffic pass, but it is not inspected by the IPS.

Step 7   Exit configuration mode.

```
router(config-if)# exit
router(config)# exit
router#
```

Step 8   Write the configuration to NVRAM.

```
router# write memory
Building configuration
[OK]
```

For More Information

- For more information on promiscuous mode, see Configuring Promiscuous Mode, page 5-15.
- For more information on inline mode, see Configuring Inline Interface Mode, page 5-16.
- For the procedure for adding the AIM IPS internal interface to the virtual sensor (vs0) so that traffic can be monitored, see Advanced Setup for the AIM IPS, page 3-12.

Establishing Sessions

Because the AIM IPS does not have an external console port, console access to the AIM IPS is enabled when you issue the **service-module ids-sensor** *slot*/*port* **session** command on the router, or when you initiate a Telnet connection into the router with the slot number corresponding to the AIM IPS port number. The lack of an external console port means that the initial bootup configuration is possible only through the router.

When you issue the **service-module ids-sensor** *slot*/*port* **session** command, you create a console session with the AIM IPS, in which you can issue any IPS configuration commands. After completing work in the session and exiting the IPS CLI, you are returned to the Cisco IOS CLI.

The **session** command starts a reverse Telnet connection using the IP address of the IDS-Sensor interface. The IDS-Sensor interface is an interface between the AIM IPS and the router. You must assign an IP address to the IDS-Sensor interface before invoking the **session** command. Assigning a routable IP address can make the IDS-Sensor interface itself vulnerable to attacks, because the AIM IPS is visible on the network through that routable IP address, meaning you can communicate with the AIM IPS outside the router. To counter this vulnerability, assign an unnumbered IP address to the IDS-Sensor interface. Then the AIM IPS IP address is only used locally between the router and the AIM IPS, and is isolated for the purposes of sessioning in to the AIM IPS.

Note   Before you install your application software or reimage the module, opening a session brings up the bootloader. After you install the software, opening a session brings up the application.

Caution   If you session to the module and perform large console transfers, character traffic may be lost unless the host console interface speed is set to 115200/bps or higher. Use the **show running config** command to check that the speed is set to 115200/bps.

For More Information

For the procedure for setting up an unnumbered IP address, see Using an Unnumbered IP Address Interface, page 17-5.

Opening and Closing a Session

Note   You must initialize the AIM IPS (run the **setup** command) from the router. After networking is configured, SSH and Telnet are available.

Use the **service-module ids-sensor** *slot/port* **session** command to establish a session from the AIM IPS to the module. Press **Ctrl-Shift-6**, then **x**, to return a session prompt to a router prompt, that is, to go from the AIM IPS prompt back to the router prompt. Press **Enter** on a blank line to go back to the session prompt, which is also the router prompt. You should only suspend a session to the router if you will be returning to the session after executing router commands. If you do not plan on returning to the AIM IPS session, you should close the session rather than suspend it.

When you close a session, you are logged completely out of the AIM IPS CLI and a new session connection requires a username and password to log in. A suspended session leaves you logged in to the CLI. When you connect with the **session** command, you can go back to the same CLI without having to provide your username and password.

Note   Telnet clients vary. In some cases, you may have to press **Ctrl-6 + x**. The control character is specified as ^^, Ctrl-^, or ASCII value 30 (hex 1E).

Caution   If you use the **disconnect** command to leave the session, the session remains running. The open session can be exploited by someone wanting to take advantage of a connection that is still in place.

To open and close sessions to the AIM IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Check the status of the AIM IPS to make sure it is running.

```
router# service-module ids-sensor 0/1 status
Service Module is Cisco IDS-Sensor0/1
Service Module supports session via TTY line 322
Service Module is in Steady state
Getting status from the Service Module, please wait..
Cisco Systems Intrusion Prevention System Network Module
  Software version:  6.1(1)E1
  Model:             AIM-IPS
  Memory:            443508 KB
  Mgmt IP addr:      10.89.148.196
  Mgmt web ports:    443
  Mgmt TLS enabled:  true


router#
```

Step 3 Open a session from the router to the AIM IPS.

```
router# service-module ids-sensor 0/1 session
Trying 10.89.148.196, 2322 ... Open
```

Step 4 Exit, or suspend and close the module session:

- sensor# **exit**

> **Note** If you are in submodes of the IPS CLI, you must exit all submodes. Enter **exit** until the sensor login prompt appears.

> ⚠ **Caution** Failing to close a session properly makes it possible for others to exploit a connection that is still in place. Remember to enter **exit** at the router# prompt to close the Cisco IOS session completely.

- To suspend and close the session to the AIM IPS, press **Ctrl-Shift** and press **6**. Release all keys, and then press **x**.

> **Note** When you are finished with a session, you need to return to the router to establish the association between a session (the IPS application) and the router interfaces you want to monitor.

Step 5 Disconnect from the router.

```
router# disconnect
```

Step 6 Press **Enter** to confirm the disconnection.

```
router# Closing connection to 10.89.148.196 [confirm] <Enter>
```

For More Information

For the procedure for initializing the AIM IPS, see Advanced Setup for the AIM IPS, page 3-12.

Displaying the Status of the AIM IPS

Use the **service-module ids-sensor** *slot/port* **status** command in privileged EXEC mode to display the status and statistics of the AIM IPS.

To display the status of the AIM IPS, follow these steps:

Step 1   Log in to the router.

Step 2   Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3   Display the status of the AIM IPS.

```
router# service-module ids-sensor 0/1 status
Service Module is Cisco IDS-Sensor0/1
Service Module supports session via TTY line 322
Service Module is in Steady state
Service Module is in fail close
Cisco Systems Intrusion Prevention System Network Module
  Software version:  6.1(1)E2
  Model:             AIM-IPS
  Memory:            443508 KB
  Mgmt IP addr:      10.89.148.196
  Mgmt web ports:    443
  Mgmt TLS enabled:  true


router#
```

Enabling and Disabling Heartbeat Reset

Use the **service-module ids-sensor** *slot/port* **heartbeat reset {enable | disable}** command in privileged EXEC mode to reset the heartbeat of the AIM IPS.

When the AIM IPS is booted in failsafe mode or is undergoing an upgrade, you can use the **service-module ids heartbeat-reset** command to prevent a reboot during the process. If you leave the heartbeat reset enabled during an upgrade, you may lose the AIM IPS heartbeat.

When the AIM IPS heartbeat is lost, the router applies a fail-open or fail-close configuration option to the AIM IPS and stops sending traffic to the AIM IPS, and sets the AIM IPS to error state. The router performs a hardware reset on the AIM IPS and monitors the AIM IPS until the heartbeat is reestablished.

Note   Disabling the heartbeat reset prevents the router from resetting the module during system image installation if the process takes too long.

To reset the heartbeat of the AIM IPS, follow these steps:

Step 1   Log in to the router.

Step 2   Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3   Verify the status of heartbeat reset.

```
router# service-module ids-sensor 0/1 status
Service Module is Cisco IDS-Sensor 0/1
Service Module supports session via TTY line 194
Service Module heartbeat-reset is enabled
```

Step 4   To disable the heartbeat on the AIM IPS:

```
router# service-module ids-sensor 0/1 heartbeat-reset disable
```

Step 5   To reenable the heartbeat on the AIM IPS:

```
router# service-module ids-sensor 0/1 heartbeat-reset enable
```

Rebooting, Resetting, and Shutting Down the AIM IPS

This section describes when and how the AIM IPS shuts down. It contains the following topics:

- AIM IPS Status Monitoring, page 17-17
- Rebooting, Resetting, and Shutting Down the AIM IPS, page 17-18

AIM IPS Status Monitoring

The AIM IPS uses RBCP to monitor its status. RBCP is monitored by the main application on the AIM IPS, not by SensorApp. If the main application on the AIM IPS fails, the RBCP heartbeat responses do not return from the AIM IPS. When the router determines that the AIM IPS has failed, a **reload** command is issued through RBCP to reboot the Linux kernel on the AIM IPS. In the period during the attempt to bring the AIM IPS back up, the router works in the mode determined by the failover operation configured.

In some cases, SensorApp may stop processing, but the main application on the AIM IPS continues to process RBCP packets. In this case, packets are processed according to the bypass settings set for the AIM IPS by the IPS CLI, IDM, or IME.

There are two situations in which the AIM IPS shuts down:

- A hardware or software error forces it to fail. The router can detect this through the loss of the RBCP heartbeat.
- **Reload** or **shutdown** command.

For More Information

- For more information on SensorApp, see SensorApp, page A-22.
- For more information on software bypass, see Configuring Inline Bypass Mode, page 5-33.

Rebooting, Resetting, and Shutting Down the AIM IPS

Use the **service-module ids-sensor** *slot/port* [**reload | reset | shutdown**] command in privileged EXEC mode to reboot, reset, and shut down the AIM IPS.

To reboot, reset, and shut down the AIM IPS, follow these steps:

Step 1   Log in to the router.

Step 2   Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3   To gracefully halt and reboot the operating system on the AIM IPS:

```
router# service-module ids-sensor 0/1 reload
Do you want to proceed with the reload? [confirm]
```

Step 4   To reset the hardware on the AIM IPS:

```
router# service-module ids-sensor 0/1 reset
Use reset only to recover from shutdown or failed state
Warning: May lose data on the hard disc!
Do you want to reset?[confirm]
```

✎ **Note**   The AIM IPS has a compact flash device that functions as a permanent storage device rather than a hard-disk drive.

⚠ **Caution**   Data loss occurs only if you issue the **reset** command without first shutting down the AIM IPS. You can use the **reset** command safely in other situations.

Step 5   To shut down applications running on the AIM IPS:

```
router# service-module ids-sensor 0/1 shutdown
Trying 10.10.10.1, 2129 . . . Open
%SERVICEMODULE-5-SHUTDOWN2:Service module IDS-Sensor1/0 shutdown complete
```

New and Modified Commands

✎ **Note**   All other Cisco IOS software commands are documented in the Cisco IOS Release 12.4(20)T command reference at Cisco.com, http://www.cisco.com/en/US/products/ps6441/index.html.

This section describes the following new and modified Cisco IOS commands, and specific commands that are used to configure the AIM IPS. This section contains the following topics:

interface ids-sensor

To configure the IPS sensor interface and enter config-if mode, use the **interface ids-sensor** command in config mode. To specify how the router handles traffic inspection during a module failure, use the **service-module** command in config-if mode. The default is fail open.

interface ids-sensor *slot/port*

ip {address | unnumbered}

service-module {*fail-close* | *fail-open*}

Syntax Description

slot	Number of the router chassis slot for the AIM IPS.
/port	Port number of the AIM IPS.
	Note The slash mark is required between the *slot* argument and the *unit* argument.
ids-sensor	The IPS interface for the sensor.
ip address	Sets the IP address of an interface.
ip unnumbered	Enables IP address processing without an explicit IP address.
service-module fail-close	The AIM IPS drops all the traffic.
service-module fail-open	The AIM IPS passes all the traffic through, but does not perform traffic inspection (default).

⚠
Caution   Although there are 57 subcommands associated with the **ip** command, the only two supported for the modules are **ip address** and ip **unnumbered**. Enabling any of the other subcommands can result in unpredictable behavior.

Command Defaults

Command Modes   Config

Config-if

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines   The **interface ids-sensor** *slot/port* command lets you enter config-if mode and configure the IPS sensor slot and port. On the AIM IPS, the slot value is 0 and the port number value is specified by identifying the physical location where the module is installed on the router.

Examples   The following example demonstrates how to use the **interface ids-sensor** command to enter config-if mode on an AIM IPS in slot 0, port1:

```
router(config)# interface ids-sensor 0/1
router(config-if)#
```

The following example demonstrates how to use the **interface ids-sensor** command with the **ip unnumbered** subcommand to specify the router command and control interface:

```
router(config)# interface ids-sensor 0/1
router(config-if)# ip unnumbered router_command_and_control_interface
router(config-if)#
```

The following example demonstrates how to use the **service-module fail-open** command to configure the module to pass all traffic through the module when the hardware fails, but not to perform traffic inspection:

```
router(config)# interface ids-sensor 0/1
router(config-if)# service-module fail-open
router(config-if)#
```

Related Commands

Command	Description
interface *interface_name*	Lets you specify which interface should be monitored.

interface *interface_name*

To enter config-if mode, configure the interface for monitoring in promiscuous or inline mode, and apply a standard or extended ACL to inline monitoring, use the **interface** *interface_name* command in config mode.

> **interface** *interface_name* **ids-service-module monitoring** {**promiscuous** | **inline**} **access-list** *number*

Syntax Description

interface_name	The name of the router interface to be monitored.
ids-service-module	Configures IPS on the interface.
monitoring	Specifies how the AIM IPS inspects traffic.
promiscuous	Specifies whether the AIM IPS inspects traffic in promiscuous mode.
inline	Specifies whether the AIM IPS inspects traffic in inline mode.
access-list	Specifies that you are applying a numbered or extended ACL to the inspected interface.
number	Number of the ACL.

Command Defaults

Command Modes   Config

Config-if

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines   The **interface** *interface_name* command lets you enter config-if mode and configure the router to operate in inline or promiscuous mode for that interface.

Examples   The following example demonstrates how to use the **interface** command to enter config-if mode and configure monitoring for GigabitEthernet0/0 using ACL 101:

```
router(config)# interface GigabitEthernet0/0
router(config-if)# ids-service-module monitoring inline access-list 101
router(config-if)#
```

Related Commands

Command	Description
interface ids-sensor	Configures the IPS interface.

service-module ids-sensor

⚠️

Caution   When you reload the router, the AIM IPS also reloads. To ensure that there is no loss of data on the AIM IPS, make sure you shut down the module using the **shutdown** command before you use the **reload** command to reboot the router.

To prevent the Cisco IOS software from rebooting the AIM IPS when the heartbeat is lost, to reboot, reset, enable console access to, shut down, see the statistics, and monitor the status of a module, use the **service-module ids-sensor** command in privileged EXEC mode.

> **service-module ids-sensor** *slot*/*port* {**heartbeat-reset** {**enable** | **disable**} **reload** | **reset** | **session** | **shutdown** | **status**}

Syntax Description

slot	Number of the router chassis slot for the AIM IPS.
/*port*	Port number of the AIM IPS.
	Note The slash mark is required between the *slot* argument and the *unit* argument.

heartbeat-reset	Enables or disables the heartbeat reset. The default is enabled.
	Note Disabling the heartbeat reset prevents the router from resetting the AIM IPS during system image installation if the process takes too long.
reload	Performs a graceful halt and reboot of the operating system on the AIM IPS.
reset	Resets the hardware on the AIM IPS. This command is usually used to recover from a shutdown.
session	Enables console access to the AIM IPS from the router.
shutdown	Shuts down the IPS application running on the AIM IPS.
statistics	Provides AIM IPS statistics.
status	Provides information about the status of the IPS software.

Defaults

Command Modes   Privileged EXEC

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was introduced.

Usage Guidelines   When the AIM IPS is booted in failsafe mode or is undergoing an upgrade, you can use the **service-module ids heartbeat-reset** command to prevent a reboot during the process. If you leave the heartbeat reset enabled during an upgrade, you may lose the AIM IPS heartbeat.

When the AIM IPS heartbeat is lost, the router applies a fail-open or fail-close configuration option to the AIM IPS and stops sending traffic to the AIM IPS, and sets the AIM IPS to error state. The router performs a hardware reset on the AIM IPS and monitors the AIM IPS until the heartbeat is reestablished.

If a confirmation prompt is displayed, press **Enter** to confirm the action or **n** to cancel.

Examples   The following example demonstrates how to disable or enable the reset action when the heartbeat is lost on an AIM IPS in slot 0, port1:

```
router# service-module ids-sensor 0/1 heartbeat-reset {disable | enable}
```

The following example demonstrates how to enable the heartbeat on the AIM IPS:

```
router# service-module ids-sensor 0/1 heartbeat-reset enable
```

The following example demonstrates how todisplay the status of the heartbeat reset by using the **service-module ids** *slot*/*port* **status** command:

```
router# service-module ids-sensor 0/1 status
Service Module is Cisco IDS-Sensor 0/1
Service Module supports session via TTY line 194
```

Service Module heartbeat-reset is enabled

The following example demonstrates how to gracefully halt and reboot the operating system on the AIM IPS:

```
router# service-module ids-sensor 0/1 reload

Do you want to proceed with reload?[confirm]
```

The following example demonstrates how to reset the hardware on an AIM IPS. A warning is displayed.

```
router# service-module ids-sensor 0/1 reset

Use reset only to recover from shutdown or failed state
Warning: May lose data on the NVRAM, nonvolatile file system or unsaved configuration!

Do you want to reset?[confirm]
```

The following example demonstrates how to enable console access to the AIM IPS operating system:

```
router# service-module ids-sensor 0/1 session
```

The following example demonstrates how to shut down IPS applications running on the AIM IPS:

```
router# service-module ids-sensor 0/1 shutdown

Trying 10.10.10.1, 2129 ... Open
%SERVICEMODULE-5-SHUTDOWN2:Service module IDS-Sensor 0/1 shutdown complete
```

The following example demonstrates how to display IPS software statistics:

```
router# service-module ids-sensor 0/1 statistics
Module Reset Statistics:
  CLI reset count = 1
  CLI reload count = 0
  Registration request timeout reset count = 1
  Error recovery timeout reset count = 1
  Module registration count = 7

The last IOS initiated event was a cli reset at 20:18:36.038 UTC Tue Jan 16 2007
```

The following example demonstrates how to display the status of the IPS software on the AIM IPS:

```
router# service-module ids-sensor 0/1 status

Service Module is Cisco IDS-Sensor0/1
Service Module supports session via TTY line 33
Service Module is in Steady state
Getting status from the Service Module, please wait...
Service Module Version information received, Major ver = 1, Minor ver= 1

Cisco Systems Intrusion Prevention System Network Module
  Software version:  6.1(1)E1
  Model:             AIM-IPS
  Memory:            890996 KB
  Mgmt IP addr:      10.1.9.201
  Mgmt web ports:    443
  Mgmt TLS enabled:  true
```

Related Commands	Command	Description
	ids-service-module monitoring	Enables IPS monitoring on a specified interface.

service-module ids-bootmode

To enter failsafe or normal boot mode for the AIM IPS, use the **service-module ids-sensor bootmode** command in privileged EXEC mode.

service-module ids-sensor *slot*/*port* **bootmode** {**failsafe** | **normal**}

Syntax Description		
	slot/	Number of the router chassis slot for the AIM IPS. The slash mark (/) is required between the *slot* argument and the *port* argument.
	port	Port number of the AIM IPS.
	failsafe	Enters failsafe boot mode on the AIM IPS .
	normal	Enters normal boot mode on the AIM IPS.

Defaults   None

Command Modes   Privileged EXEC (#)

Command History	Release	Modification
	12.4(15)XY	This command was introduced.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines   If a confirmation prompt is displayed, press **Enter** to confirm the action, or press **n** to cancel.

Examples   The following example demonstrates how to enter failsafe boot mode on an AIM IPS in slot 0, port 1:

```
router# service-module ids-sensor 0/1 bootmode failsafe
```

The following example demonstrates how to enter normal boot mode on the AIM IPS:

```
router# service-module ids-sensor 0/1 bootmode normal
```

Related Commands	Command	Description
	ids-service-module monitoring	Enables IDS monitoring on a specified interface.