Configuring the ASA IPS Module

This chapter describes how to configure the ASA IPS module. The ASA IPS module might be a hardware module or a software module, depending on your ASA model. For a list of supported ASA IPS modules per ASA model, see the *Cisco ASA Compatibility Matrix*:

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

This chapter includes the following sections:

Information About the ASA IPS Module

The ASA IPS module runs advanced IPS software that provides proactive, full-featured intrusion prevention services to stop malicious traffic, including worms and network viruses, before they can affect your network. This section includes the following topics:

How the ASA IPS Module Works with the ASA

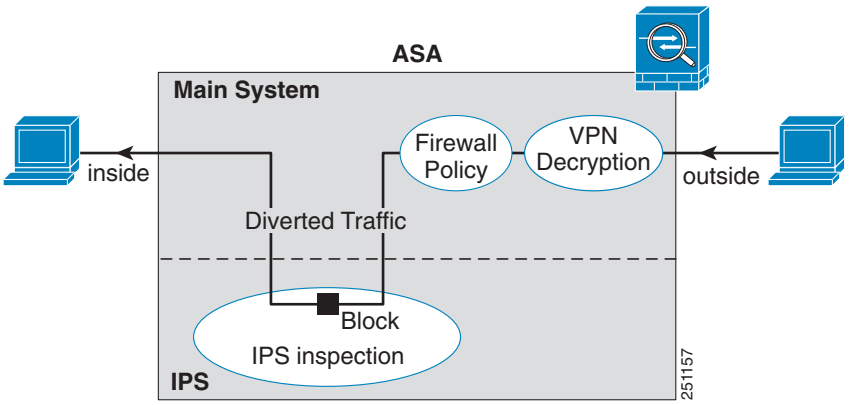
The ASA IPS module runs a separate application from the ASA. The ASA IPS module might include an external management interface so you can connect to the ASA IPS module directly; if it does not have a management interface, you can connect to the ASA IPS module through the ASA interface. The ASA IPS SSP on the ASA 5585-X includes data interfaces; these interfaces provide additional port-density for the ASA. However, the overall through-put of the ASA is not increased.

Traffic goes through the firewall checks before being forwarded to the ASA IPS module. When you identify traffic for IPS inspection on the ASA, traffic flows through the ASA and the ASA IPS module as follows. **Note**: This example is for "inline mode." See the "Operating Modes" section on page 31-3 for information about "promiscuous mode," where the ASA only sends a copy of the traffic to the ASA IPS module.

1. Traffic enters the ASA.
2. Incoming VPN traffic is decrypted.
3. Firewall policies are applied.
4. Traffic is sent to the ASA IPS module.
5. The ASA IPS module applies its security policy to the traffic, and takes appropriate actions.
6. Valid traffic is sent back to the ASA; the ASA IPS module might block some traffic according to its security policy, and that traffic is not passed on.
7. Outgoing VPN traffic is encrypted.
8. Traffic exits the ASA.

Figure 31-1 shows the traffic flow when running the ASA IPS module in inline mode. In this example, the ASA IPS module automatically blocks traffic that it identified as an attack. All other traffic is forwarded through the ASA.

Figure 31-1 ASA IPS module Traffic Flow in the ASA: Inline Mode

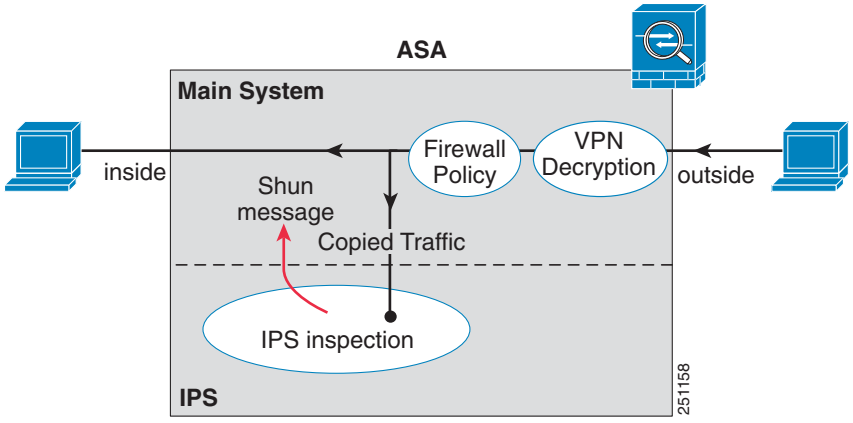


Operating Modes

You can send traffic to the ASA IPS module using one of the following modes:

- Inline mode—This mode places the ASA IPS module directly in the traffic flow (see Figure 31-1). No traffic that you identified for IPS inspection can continue through the ASA without first passing through, and being inspected by, the ASA IPS module. This mode is the most secure because every packet that you identify for inspection is analyzed before being allowed through. Also, the ASA IPS module can implement a blocking policy on a packet-by-packet basis. This mode, however, can affect throughput.
- Promiscuous mode—This mode sends a duplicate stream of traffic to the ASA IPS module. This mode is less secure, but has little impact on traffic throughput. Unlike inline mode, in promiscuous mode the ASA IPS module can only block traffic by instructing the ASA to shun the traffic or by resetting a connection on the ASA. Also, while the ASA IPS module is analyzing the traffic, a small amount of traffic might pass through the ASA before the ASA IPS module can shun it. Figure 31-2 shows the ASA IPS module in promiscuous mode. In this example, the ASA IPS module sends a shun message to the ASA for traffic it identified as a threat.

Figure 31-2 ASA IPS module Traffic Flow in the ASA: Promiscuous Mode



Using Virtual Sensors (ASA 5510 and Higher)

The ASA IPS module running IPS software Version 6.0 and later can run multiple virtual sensors, which means you can configure multiple security policies on the ASA IPS module. You can assign each ASA security context or single mode ASA to one or more virtual sensors, or you can assign multiple security contexts to the same virtual sensor. See the IPS documentation for more information about virtual sensors, including the maximum number of sensors supported.

Figure 31-3 shows one security context paired with one virtual sensor (in inline mode), while two security contexts share the same virtual sensor.

Figure 31-3 Security Contexts and Virtual Sensors

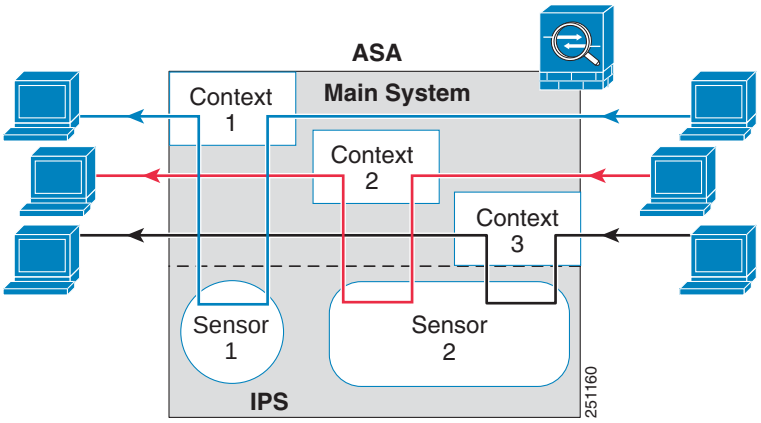
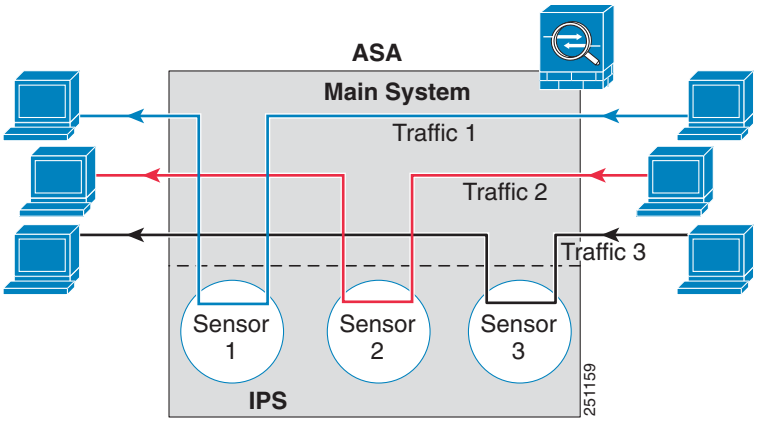


Figure 31-4 shows a single mode ASA paired with multiple virtual sensors (in inline mode); each defined traffic flow goes to a different sensor.

Figure 31-4 Single Mode ASA with Multiple Virtual Sensors



Information About Management Access

You can manage the IPS application using the following methods:

- Sessioning to the module from the ASA—If you have CLI access to the ASA, then you can session to the module and access the module CLI. See the "Sessioning to the Module from the ASA" section on page 31-11.
- Connecting to the IPS management interface using ASDM or SSH—After you launch ASDM from the ASA, your management station connects to the module management interface to configure the IPS application. For SSH, you can access the module CLI directly on the module management interface. (Telnet access requires additional configuration in the module application). The module management interface can also be used for sending syslog messages or allowing updates for the module application, such as signature database updates.

See the following information about the management interface:

- ASA 5510, ASA 5520, ASA 5540, ASA 5580, ASA 5585-X—The IPS management interface is a separate external Gigabit Ethernet interface.
- ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X—These models run the ASA IPS module as a software module. The IPS management interface shares the Management 0/0 interface with the ASA. Separate MAC addresses and IP addresses are supported for the ASA and ASA IPS module. You must perform configuration of the IPS IP address within the IPS operating system (using the CLI or ASDM). However, physical characteristics (such as enabling the interface) are configured on the ASA. You can remove the ASA interface configuration (specifically the interface name) to dedicate this interface as an IPS-only interface. This interface is management-only.
- ASA 5505—You can use an ASA VLAN to allow access to an internal management IP address over the backplane.

Licensing Requirements for the ASA IPS module

The following table shows the licensing requirements for this feature:

Model	License Requirement
ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	IPS Module License. **Note** The IPS module license lets you run the IPS software module on the ASA. You must also purchase a separate IPS signature subscription; for failover, purchase a subscription for each unit. To obtain IPS signature support, you must purchase the ASA with IPS pre-installed (the part number must include "IPS"). The combined failover cluster license does not let you pair non-IPS and IPS units. For example, if you buy the IPS version of the ASA 5515-X (part number ASA5515-IPS-K9) and try to make a failover pair with a non-IPS version (part number ASA5515-K9), then you will not be able to obtain IPS signature updates for the ASA5515-K9 unit, even though it has an IPS module license inherited from the other unit.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

The ASA 5505 does not support multiple context mode, so multiple context features, such as virtual sensors, are not supported on the AIP SSC.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

Model Guidelines

- See the *Cisco ASA Compatibility Matrix* for information about which models support which modules:

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- The ASA 5505 does not support multiple context mode, so multiple context features, such as virtual sensors, are not supported on the AIP SSC.
- The ASA IPS module for the ASA 5510 and higher supports higher performance requirements, while the ASA IPS module for the ASA 5505 is designed for a small office installation. The following features are not supported for the ASA 5505:
  - Virtual sensors
  - Anomaly detection
  - Unretirement of default retired signatures

Additional Guidelines

- The total throughput for the ASA plus the IPS module is lower than ASA throughput alone.
  - ASA 5512-X through ASA 5555-X—See http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-700608.html
  - ASA 5585-X—See http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-617018.html
  - ASA 5505 through ASA 5540—See http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html
- You cannot change the software type installed on the module; if you purchase an ASA IPS module, you cannot later install other software on it.

Default Settings

Table 31-1 lists the default settings for the ASA IPS module.

Table 31-1 Default Network Parameters

Parameters	Default
Management VLAN (ASA 5505 only)	VLAN 1
Management IP address	192.168.1.2/24
Gateway	192.168.1.1/24 (the default ASA management IP address)
Username	cisco
Password	cisco

Note The default management IP address on the ASA is 192.168.1.1/24.

Configuring the ASA IPS module

This section describes how to configure the ASA IPS module and includes the following topics:

Task Flow for the ASA IPS Module

Configuring the ASA IPS module is a process that includes configuration of the IPS security policy on the ASA IPS module and then configuration of the ASA to send traffic to the ASA IPS module. To configure the ASA IPS module, perform the following steps:

Step 1 Cable the ASA IPS management interface. See the "Connecting the ASA IPS Management Interface" section on page 31-8.

Step 2 Session to the module. Access the IPS CLI over the backplane.See the "Sessioning to the Module from the ASA" section on page 31-11.

Step 3 (ASA 5512-X through ASA 5555-X; may be required) Install the software module. See the "(ASA 5512-X through ASA 5555-X) Booting the Software Module" section on page 31-11.

Step 4 Depending on your ASA model:

- (ASA 5510 and higher) Configure basic network settings for the IPS module. See the "(ASA 5510 and Higher) Configuring Basic Network Settings" section on page 31-13.
- (ASA 5505) Configure the management VLAN and IP address for the IPS module. See the "(ASA 5505) Configuring Basic Network Settings" section on page 31-13.

Step 5 On the module, configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. See the "Configuring the Security Policy on the ASA IPS Module" section on page 31-15.

Step 6 (ASA 5510 and higher, optional) On the ASA in multiple context mode, specify which IPS virtual sensors are available for each context (if you configured virtual sensors). See the "Assigning Virtual Sensors to a Security Context (ASA 5510 and Higher)" section on page 31-16.

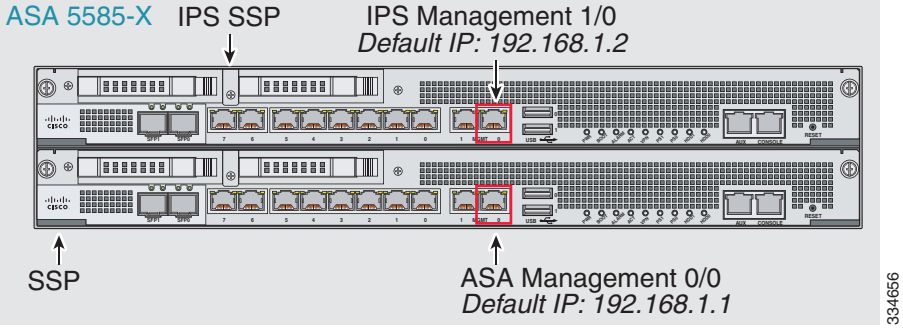
Step 7 On the ASA, identify traffic to divert to the ASA IPS module. See the "Diverting Traffic to the ASA IPS module" section on page 31-18.

Connecting the ASA IPS Management Interface

In addition to providing management access to the IPS module, the IPS management interface needs access to an HTTP proxy server or a DNS server and the Internet so it can download global correlation, signature updates, and license requests. This section describes recommended network configurations. Your network may differ.

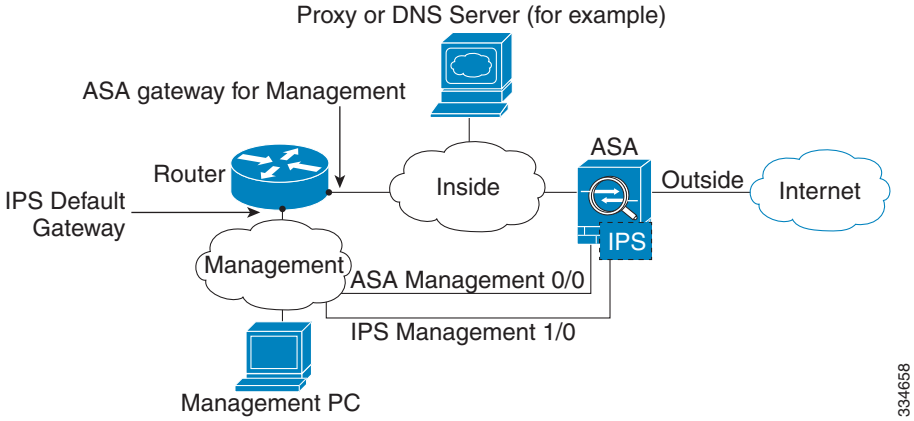
ASA 5510, ASA 5520, ASA 5540, ASA 5580, ASA 5585-X (Hardware Module)

The IPS module includes a separate management interface from the ASA.



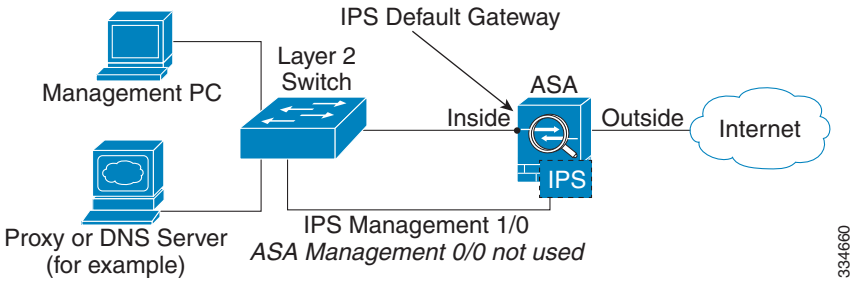
If you have an inside router

If you have an inside router, you can route between the management network, which can include both the ASA Management 0/0 and IPS Management 1/0 interfaces, and the ASA inside network. Be sure to also add a route on the ASA to reach the Management network through the inside router.



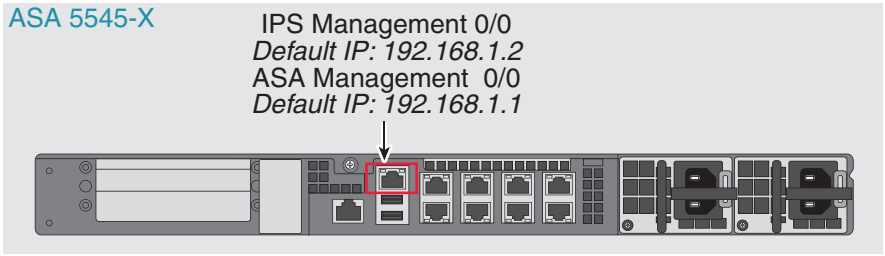
If you do not have an inside router

If you have only one inside network, then you cannot also have a separate management network, which would require an inside router to route between the networks. In this case, you can manage the ASA from the inside interface instead of the Management 0/0 interface. Because the IPS module is a separate device from the ASA, you can configure the IPS Management 1/0 address to be on the same network as the inside interface.



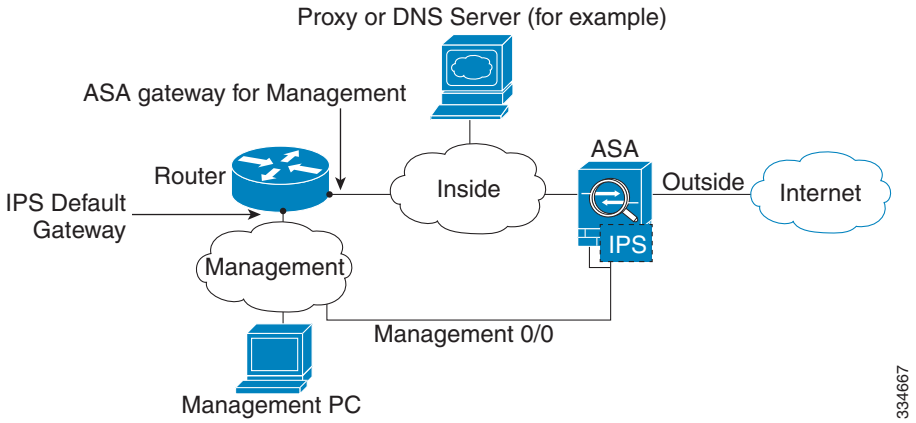
ASA 5512-X through ASA 5555-X (Software Module)

These models run the IPS module as a software module, and the IPS management interface shares the Management 0/0 interface with the ASA.



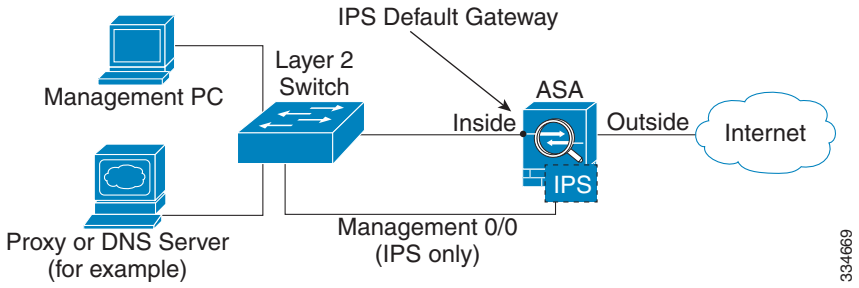
If you have an inside router

If you have an inside router, you can route between the Management 0/0 network, which includes both the ASA and IPS management IP addresses, and the inside network. Be sure to also add a route on the ASA to reach the Management network through the inside router.



If you do not have an inside router

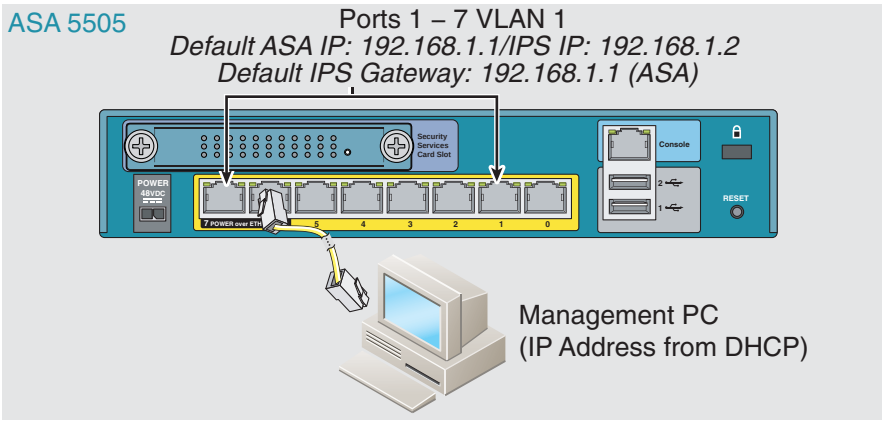
If you have only one inside network, then you cannot also have a separate management network. In this case, you can manage the ASA from the inside interface instead of the Management 0/0 interface. If you remove the ASA-configured name from the Management 0/0 interface, you can still configure the IPS IP address for that interface. Because the IPS module is essentially a separate device from the ASA, you *can* configure the IPS management address to be on the same network as the inside interface.



Note You must remove the ASA-configured name for Management 0/0; if it is configured on the ASA, then the IPS address must be on the same network as the ASA, and that excludes any networks already configured on other ASA interfaces. If the name is not configured, then the IPS address can be on any network, for example, the ASA inside network.

ASA 5505

The ASA 5505 does not have a dedicated management interface. You must use an ASA VLAN to access an internal management IP address over the backplane. Connect the management PC to one of the following ports: Ethernet 0/1 through 0/7, which are assigned to VLAN 1.



What to Do Next

- (ASA 5510 and higher) Configure basic network settings. See the "(ASA 5510 and Higher) Configuring Basic Network Settings" section on page 31-13.
- (ASA 5505) Configure management interface settings. See the "(ASA 5505) Configuring Basic Network Settings" section on page 31-13.

Sessioning to the Module from the ASA

To access the IPS module CLI from the ASA, you can session from the ASA. For software modules, you can either session to the module (using Telnet) or create a virtual console session. A console session might be useful if the control plane is down and you cannot establish a Telnet session.

Detailed Steps

Command	Purpose

Telnet session.
For a hardware module (for example, the ASA 5585-X):
session 1
For a software module (for example, the ASA 5545-X):
session ips
 	
Example:
`ciscoasa# session 1`
 	
`Opening command session with slot 1.`
`Connected to slot 1. Escape character sequence is 'CTRL-^X'.`
 	
`sensor login: cisco`
`Password: cisco`
	Accesses the module using Telnet. You are prompted for the username and password. The default username is **cisco**, and the default password is **cisco**.
	Note The first time you log in to the module, you are prompted to change the default password. Passwords must be at least eight characters long and cannot be a word in the dictionary.

Console session (software module only).
session ips console
 	
Example:
`ciscoasa# session ips console`
 	
`Establishing console session with slot 1`
`Opening console session with module ips.`
`Connected to module ips. Escape character sequence is 'CTRL-SHIFT-6 then x'.`
 	
`sensor login: cisco`
`Password: cisco`
	Accesses the module console. You are prompted for the username and password. The default username is **cisco**, and the default password is **cisco**.
	Note Do not use this command in conjunction with a terminal server where **Ctrl-Shift-6, x** is the escape sequence to return to the terminal server prompt. **Ctrl-Shift-6, x** is also the sequence to escape the IPS console and return to the ASA prompt. Therefore, if you try to exit the IPS console in this situation, you instead exit all the way to the terminal server prompt. If you reconnect the terminal server to the ASA, the IPS console session is still active; you can never exit to the ASA prompt. You must use a direct serial connection to return the console to the ASA prompt.
	
	Use the **session ips** command instead.

(ASA 5512-X through ASA 5555-X) Booting the Software Module

Your ASA typically ships with IPS module software present on Disk0. If the module is not running, or if you are adding the IPS module to an existing ASA, you must boot the module software. If you are unsure if the module is running, you will not be able to session it.

Detailed Steps

Step 1 Do one of the following:

- New ASA with IPS pre-installed—To view the IPS module software filename in flash memory, enter:.

  ```
  ciscoasa# dir disk0:
  ```

  For example, look for a filename like IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip. Note the filename; you will need this filename later in the procedure.

- Existing ASA with new IPS installation—Download the IPS software from Cisco.com to a TFTP server. If you have a Cisco.com login, you can obtain the software from the following website:

  http://www.cisco.com/cisco/software/navigator.html?mdfid=282164240

  Copy the software to the ASA:

  ```
  ciscoasa# copy tftp://server/file_path disk0:/file_path
  ```

  For other download server types, see Chapter 46, "Managing Software and Configurations," in the general operations configuration guide.

  Note the filename; you will need this filename later in the procedure.

Step 2 To set the IPS module software location in disk0, enter the following command:

```
ciscoasa# sw-module module ips recover configure image disk0:file_path
```

For example, using the filename in the example in Step 1, enter:

```
ciscoasa# sw-module module ips recover configure image
disk0:IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip
```

Step 3 To install and load the IPS module software, enter the following command:

```
ciscoasa# sw-module module ips recover boot
```

Step 4 To check the progress of the image transfer and module restart process, enter the following command:

```
ciscoasa# show module ips details
```

The Status field in the output indicates the operational status of the module. A module operating normally shows a status of "Up." While the ASA transfers an application image to the module, the Status field in the output reads "Recover." When the ASA completes the image transfer and restarts the module, the newly transferred image is running.

Configuring Basic IPS Module Network Settings

(ASA 5510 and Higher) Configuring Basic Network Settings

Session to the module from the ASA and configure basic settings using the **setup** command.

Note (ASA 5512-X through ASA 5555-X) If you cannot session to the module, then the IPS module is not running. See the "(ASA 5512-X through ASA 5555-X) Booting the Software Module" section on page 31-11, and then repeat this procedure after you install the module.

Detailed Steps

	Command	Purpose
Step 1	Session to the IPS module according to the "Sessioning to the Module from the ASA" section on page 31-11.	

Step 2	`setup`
	
	Example:
	`sensor# setup`
		Runs the setup utility for initial configuration of the ASA IPS module. You are prompted for basic settings. For the default gateway, specify the IP address of the upstream router. See the "Connecting the ASA IPS Management Interface" section on page 31-8 to understand the requirements for your network. The default setting of the ASA management IP address will not work.

(ASA 5505) Configuring Basic Network Settings

An ASA IPS module on the ASA 5505 does not have any external interfaces. You can configure a VLAN to allow access to an internal IPS management IP address over the backplane. By default, VLAN 1 is enabled for IPS management. You can only assign one VLAN as the management VLAN. This section describes how to change the management VLAN and IP address if you do not want to use the default, and how to set other required network parameters.

Note Perform this configuration on the ASA 5505, not on the ASA IPS module.

Prerequisites

When you change the IPS VLAN and management address from the default, be sure to also configure the matching ASA VLAN and switch port(s) according to the procedures listed in Chapter 12, "Starting Interface Configuration (ASA 5505)," in the general operations configuration guide. You must define and configure the VLAN for the ASA so the IPS management interface is accessible on the network.

Restrictions

Do not configure NAT for the management address if you intend to access it using ASDM. For initial setup with ASDM, you need to access the real address. After initial setup (where you set the password on the ASA IPS module), you can configure NAT and supply ASDM with the translated address for accessing the ASA IPS module.

Detailed Steps

	Command	Purpose
Step 1	**interface vlan** *number* **Example:** `ciscoasa(config)# interface vlan 1`	Specifies the current management VLAN for which you want to disable IPS management. By default, this is VLAN 1.
Step 2	**no allow-ssc-mgmt** **Example:** `ciscoasa(config-if)# no allow-ssc-mgmt`	Disables IPS management for the old VLAN so that you can enable it for a different VLAN.
Step 3	**interface vlan** *number* **Example:** `ciscoasa(config)# interface vlan 20`	Specifies the VLAN you want to use as the new IPS management VLAN.
Step 4	**allow-ssc-mgmt** **Example:** `ciscoasa(config-if)# allow-ssc-mgmt`	Sets this interface as the IPS management interface.

	Command	Purpose
Step 5	**hw-module module 1 ip** *ip_address netmask gateway* **Example:** `ciscoasa# hw-module module 1 ip 10.1.1.2 255.255.255.0 10.1.1.1`	Configures the management IP address for the ASA IPS module. Make sure this address is on the same subnet as the ASA VLAN IP address. For example, if you assigned 10.1.1.1 to the VLAN for the ASA, then assign another address on that network, such as 10.1.1.2, for the IPS management address. Set the gateway to be the ASA IP address for the management VLAN. By default, this IP address is 192.168.1.1. **Note** These settings are written to the IPS application configuration, not the ASA configuration. You can view these settings from the ASA using the **show module details** command. You can alternatively use the IPS application **setup** command to configure this setting from the IPS CLI.
Step 6	**hw-module module 1 allow-ip** *ip_address netmask* **Example:** `ciscoasa# hw-module module 1 allow-ip 10.1.1.30 255.255.255.0`	Sets the hosts that are allowed to access the management IP address. **Note** These settings are written to the IPS application configuration, not the ASA configuration. You can view these settings from the ASA using the **show module details** command. You can alternatively use the IPS application **setup** command to configure this setting from the IPS CLI.

Examples

The following example configures VLAN 20 as the IPS management VLAN. Only the host at 10.1.1.30 can access the IPS management IP address. VLAN 20 is assigned to switch port Ethernet 0/0. When you connect to ASDM on ASA interface 10.1.1.1, ASDM then accesses the IPS on 10.1.1.2.

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# no allow-ssc-mgmt

ciscoasa(config-if)# interface vlan 20
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# allow-ssc-mgmt
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# hw-module module 1 ip 10.1.1.2 255.255.255.0 10.1.1.1
ciscoasa(config)# hw-module module 1 allow-ip 10.1.1.30 255.255.255.255

ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 20
ciscoasa(config-if)# no shutdown
```

Configuring the Security Policy on the ASA IPS Module

This section describes how to configure the ASA IPS module application.

Detailed Steps

Step 1 Access the ASA IPS module CLI using one of the following methods:

- Session from the ASA to the ASA IPS module. See the "Sessioning to the Module from the ASA" section on page 31-11.
- Connect to the IPS management interface using SSH. If you did not change it, the default management IP address is 192.168.1.2. The default username is **cisco**, and the default password is **cisco**. See the "Information About Management Access" section on page 31-4 for more information about the management interface.

Step 2 Configure the IPS security policy according to the IPS documentation.

To access all documents related to IPS, go to: http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_documentation_roadmaps_list.html

Step 3 (ASA 5510 and higher) If you configure virtual sensors, you identify one of the sensors as the default. If the ASA does not specify a virtual sensor name in its configuration, the default sensor is used.

Step 4 When you are done configuring the ASA IPS module, exit the IPS software by entering the following command:

```
sensor# exit
```

If you sessioned to the ASA IPS module from the ASA, you return to the ASA prompt.

What to Do Next

- For the ASA in multiple context mode, see the "Assigning Virtual Sensors to a Security Context (ASA 5510 and Higher)" section on page 31-16.
- For the ASA in single context mode, see the "Diverting Traffic to the ASA IPS module" section on page 31-18.

Assigning Virtual Sensors to a Security Context (ASA 5510 and Higher)

If the ASA is in multiple context mode, then you can assign one or more IPS virtual sensors to each context. Then, when you configure the context to send traffic to the ASA IPS module, you can specify a sensor that is assigned to the context; you cannot specify a sensor that you did not assign to the context. If you do not assign any sensors to a context, then the default sensor configured on the ASA IPS module is used. You can assign the same sensor to multiple contexts.

Note You do not need to be in multiple context mode to use virtual sensors; you can be in single mode and use different sensors for different traffic flows.

Prerequisites

For more information about configuring contexts, see the "Configuring Multiple Contexts" section on page 8-15 in the general operations configuration guide.

Detailed Steps

	Command	Purpose

Step 1	**context** *name*
	
	Example:
	`ciscoasa(config)# context admin`
	`ciscoasa(config-ctx)#`
		Identifies the context you want to configure. Enter this command in the system execution space.

Step 2	**allocate-ips** *sensor_name* [*mapped_name*] [**default**] **Example:** `ciscoasa(config-ctx)# allocate-ips sensor1 highsec`	Enter this command for each sensor you want to assign to the context. The *sensor _name* argument is the sensor name configured on the ASA IPS module. To view the sensors that are configured on the ASA IPS module, enter **allocate-ips ?**. All available sensors are listed. You can also enter the **show ips** command. In the system execution space, the **show ips** command lists all available sensors; if you enter it in the context, it shows the sensors you already assigned to the context. If you specify a sensor name that does not yet exist on the ASA IPS module, you get an error, but the **allocate-ips** command is entered as is. Until you create a sensor of that name on the ASA IPS module, the context assumes the sensor is down. Use the *mapped_name* argument as an alias for the sensor name that can be used within the context instead of the actual sensor name. If you do not specify a mapped name, the sensor name is used within the context. For security purposes, you might not want the context administrator to know which sensors are being used by the context. Or you might want to genericize the context configuration. For example, if you want all contexts to use sensors called “sensor1” and “sensor2,” then you can map the “highsec” and “lowsec” sensors to sensor1 and sensor2 in context A, but map the “medsec” and “lowsec” sensors to sensor1 and sensor2 in context B. The **default** keyword sets one sensor per context as the default sensor; if the context configuration does not specify a sensor name, the context uses this default sensor. You can only configure one default sensor per context. If you want to change the default sensor, enter the **no allocate-ips** *sensor_name* command to remove the current default sensor before you allocate a new default sensor. If you do not specify a sensor as the default, and the context configuration does not include a sensor name, then traffic uses the default sensor as specified on the ASA IPS module.

Step 3	**changeto context** *context_name*
	
	Example:
	`ciscoasa# changeto context customer1`
	`ciscoasa/customer1#`
		Changes to the context so you can configure the IPS security policy as described in “Diverting Traffic to the ASA IPS module” section on page 31-18.

Examples

The following example assigns sensor1 and sensor2 to context A, and sensor1 and sensor3 to context B. Both contexts map the sensor names to "ips1" and "ips2." In context A, sensor1 is set as the default sensor, but in context B, no default is set so the default that is configured on the ASA IPS module is used.

```
ciscoasa(config-ctx)# context A
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1 default
ciscoasa(config-ctx)# allocate-ips sensor2 ips2
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1
ciscoasa(config-ctx)# allocate-ips sensor3 ips2
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver

ciscoasa(config-ctx)# changeto context A
...
```

What to Do Next

Change to each context to configure the IPS security policy as described in "Diverting Traffic to the ASA IPS module" section on page 31-18.

Diverting Traffic to the ASA IPS module

This section identifies traffic to divert from the ASA to the ASA IPS module.

Prerequisites

In multiple context mode, perform these steps in each context execution space. To change to a context, enter the **changeto context** *context_name* command.

Detailed Steps

	Command	Purpose
Step 1	**class-map** *name* **Example:** `ciscoasa(config)# class-map ips_class`	Creates a class map to identify the traffic for which you want to send to the ASA IPS module. If you want to send multiple traffic classes to the ASA IPS module, you can create multiple class maps for use in the security policy.
Step 2	**match** *parameter* **Example:** `ciscoasa(config-cmap)# match access-list ips_traffic`	Specifies the traffic in the class map. See the "Identifying Traffic (Layer 3/4 Class Maps)" section on page 1-12 for more information.
Step 3	**policy-map** *name* **Example:** `ciscoasa(config)# policy-map ips_policy`	Adds or edits a policy map that sets the actions to take with the class map traffic.
Step 4	**class** *name* **Example:** `ciscoasa(config-pmap)# class ips_class`	Identifies the class map you created in Step 1.

	Command	Purpose
Step 5	**ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}] **Example:** `ciscoasa(config-pmap-c)# ips promiscuous fail-close`	Specifies that the traffic should be sent to the ASA IPS module. The **inline** and **promiscuous** keywords control the operating mode of the ASA IPS module. See the "Operating Modes" section on page 31-3 for more details. The **fail-close** keyword sets the ASA to block all traffic if the ASA IPS module is unavailable. The **fail-open** keyword sets the ASA to allow all traffic through, uninspected, if the ASA IPS module is unavailable. (ASA 5510 and higher) If you use virtual sensors, you can specify a sensor name using the **sensor** *sensor_name* argument. To see available sensor names, enter the **ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} **sensor ?** command. Available sensors are listed. You can also use the **show ips** command. If you use multiple context mode on the ASA, you can only specify sensors that you assigned to the context (see the "Assigning Virtual Sensors to a Security Context (ASA 5510 and Higher)" section on page 31-16). Use the *mapped_name* if configured in the context. If you do not specify a sensor name, then the traffic uses the default sensor. In multiple context mode, you can specify a default sensor for the context. In single mode or if you do not specify a default sensor in multiple mode, the traffic uses the default sensor that is set on the ASA IPS module. If you enter a name that does not yet exist on the ASA IPS module, you get an error, and the command is rejected.
Step 6	(Optional) **class** *name2* **Example:** `ciscoasa(config-pmap)# class ips_class2`	If you created multiple class maps for IPS traffic, you can specify another class for the policy. See the "Feature Matching Within a Service Policy" section on page 1-3 for detailed information about how the order of classes matters within a policy map. Traffic cannot match more than one class map for the same action type; so if you want network A to go to sensorA, but want all other traffic to go to sensorB, then you need to enter the **class** command for network A before you enter the **class** command for all traffic; otherwise all traffic (including network A) will match the first **class** command, and will be sent to sensorB.

	Command	Purpose
Step 7	(Optional) **ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}] **Example:** `ciscoasa(config-pmap-c)# ips promiscuous fail-close`	Specifies that the second class of traffic should be sent to the ASA IPS module. Add as many classes as desired by repeating these steps.
Step 8	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **Example:** `ciscoasa(config)# service-policy tcp_bypass_policy outside`	Activates the policy map on one or more interfaces. **global** applies the policy map to all interfaces, and **interface** applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

Managing the ASA IPS module

This section includes procedures that help you recover or troubleshoot the module and includes the following topics:

Installing and Booting an Image on the Module

If the module suffers a failure, and the module application image cannot run, you can reinstall a new image on the module from a TFTP server (for a hardware module), or from the local disk (software module).

Note Do not use the **upgrade** command within the module software to install the image.

Prerequisites

- Hardware module—Be sure the TFTP server that you specify can transfer files up to 60 MB in size.

  Note This process can take approximately 15 minutes to complete, depending on your network and the size of the image.

- Software module—Copy the image to the ASA internal flash (disk0) before completing this procedure.

Note Before you download the IPS software to disk0, make sure at least 50% of the flash memory is free. When you install IPS, IPS reserves 50% of the internal flash memory for its file system.

Detailed Steps

	Command	Purpose

Step 1	For a hardware module (for example, the ASA 5585-X):
	hw-module module 1 recover configure
	For a software module (for example, the ASA 5545-X):
	sw-module module ips recover configure image disk0:*file_path*
	Example:
	`ciscoasa# hw-module module 1 recover configure`
	`Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg`
	`Port IP Address [127.0.0.2]: 10.1.2.10`
	`Port Mask [255.255.255.254]: 255.255.255.0`
	`Gateway IP Address [1.1.2.10]: 10.1.2.254`
	`VLAN ID [0]: 100`
		Specifies the location of the new image.
		For a hardware module—This command prompts you for the URL for the TFTP server, the management interface IP address and netmask, gateway address, and VLAN ID (ASA 5505 only). These network parameters are configured in ROMMON; the network parameters you configured in the module application configuration are not available to ROMMON, so you must set them separately here.
		For a software module—Specify the location of the image on the local disk.
		You can view the recovery configuration using the **show module** {**1** | **ips**} **recover** command.
		In multiple context mode, enter this command in the system execution space.

Step 2	For a hardware module: **hw-module module 1 recover boot** For a software module: **sw-module module ips recover boot** **Example:** `ciscoasa# hw-module module 1 recover boot`	Installs and boots the IPS module software.
Step 3	For a hardware module: **show module 1 details** For a software module: **show module ips details** **Example:** `ciscoasa# show module 1 details`	Checks the progress of the image transfer and module restart process. The Status field in the output indicates the operational status of the module. A module operating normally shows a status of "Up." While the ASA transfers an application image to the module, the Status field in the output reads "Recover." When the ASA completes the image transfer and restarts the module, the newly transferred image is running.

Shutting Down the Module

Shutting down the module software prepares the module to be safely powered off without losing configuration data. **Note**: If you reload the ASA, the module is not automatically shut down, so we recommend shutting down the module before reloading the ASA. To gracefully shut down the module, perform the following steps at the ASA CLI.

Detailed Steps

Command	Purpose
For a hardware module (for example, the ASA 5585-X): **hw-module module 1 shutdown** For a software module (for example, the ASA 5545-X): **sw-module module ips shutdown** **Example:** `ciscoasa# hw-module module 1 shutdown`	Shuts down the module.

Uninstalling a Software Module Image

To uninstall a software module image and associated configuration, perform the following steps.

Detailed Steps

	Command	Purpose

Step 1	**sw-module module ips uninstall**
	Example:
	`ciscoasa# sw-module module ips uninstall`
	`Module ips will be uninstalled. This will completely remove the`
	`disk image associated with the sw-module including any configuration`
	`that existed within it.`
	`Uninstall module <id>? [confirm]`
		Permanently uninstalls the software module image and associated configuration.

Step 2	**reload** **Example:** `ciscoasa# reload`	Reloads the ASA. You must reload the ASA before you can install a new module type.

Resetting the Password

You can reset the module password to the default. For the user **cisco**, the default password is **cisco**. After resetting the password, you should change it to a unique value using the module application.

Resetting the module password causes the module to reboot. Services are not available while the module is rebooting.

To reset the module password to the default of cisco, perform the following steps.

Detailed Steps

Command	Purpose
For a hardware module (for example, the ASA 5585-X): **hw-module module 1 password-reset** For a software module (for example, the ASA 5545-X): **sw-module module ips password-reset** **Example:** `ciscoasa# hw-module module 1 password-reset`	Resets the module password to **cisco** for user **cisco**.

Reloading or Resetting the Module

To reload or reset the module, enter one of the following commands at the ASA CLI.

Detailed Steps

Command	Purpose
For a hardware module (for example, the ASA 5585-X): **hw-module module 1 reload** For a software module (for example, the ASA 5545-X): **sw-module module ips reload** **Example:** `ciscoasa# hw-module module 1 reload`	Reloads the module software.
For a hardware module: **hw-module module 1 reset** For a software module: **sw-module module ips reset** **Example:** `ciscoasa# hw-module module 1 reset`	Performs a reset, and then reloads the module.

Monitoring the ASA IPS module

To check the status of a module, enter one of the following commands:

Command	Purpose
show module	Displays the status.
show module {**1** | **ips**} **details**	Displays additional status information. Specify **1** for a hardware module and **ips** for a software module.
show module {**1** | **ips**} **recover**	Displays the network parameters for transferring an image to the module. Specify **1** for a hardware module and **ips** for a software module.

Examples

The following is sample output from the **show module details** command, which provides additional information for an ASA with an SSC installed:

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Card-5
Hardware version: 0.1
```

```
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App. Name: IPS
App. Status: Up
App. Status Desc: Not Applicable
App. Version: 6.2(1)E2
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
                  209.165.202.158/32
                  209.165.200.254/24
Mgmt Vlan: 20
```

The following is sample output from the **show module ips** command for an ASA 5525-X with an IPS SSP software module installed:

```
ciscoasa# show module ips
Mod Card Type                                    Model           Serial No.
--- -------------------------------------------- ------------------------------
ips IPS 5525 Intrusion Protection System         IPS5525         FCH1504V03P

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ---------------------------
ips 503d.e59c.6f89 to 503d.e59c.6f89  N/A          N/A          7.1(1.160)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ----------------------------------------
ips IPS                            Up               7.1(1.160)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
ips Up                 Up

Mod License Name      License Status  Time Remaining
--- ----------------- --------------- ---------------
ips IPS Module        Enabled         7 days
```

Configuration Examples for the ASA IPS module

The following example diverts all IP traffic to the ASA IPS module in promiscuous mode, and blocks all IP traffic if the ASA IPS module card fails for any reason:

```
ciscoasa(config)# access-list IPS permit ip any any
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list IPS
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips promiscuous fail-close
ciscoasa(config-pmap-c)# service-policy my-ips-policy global
```

The following example diverts all IP traffic destined for the 10.1.1.0 network and the 10.2.1.0 network to the AIP SSM in inline mode, and allows all traffic through if the AIP SSM fails for any reason. For the my-ips-class traffic, sensor1 is used; for the my-ips-class2 traffic, sensor2 is used.

```
ciscoasa(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
```

```
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list my-ips-acl
ciscoasa(config)# class-map my-ips-class2
ciscoasa(config-cmap)# match access-list my-ips-acl2
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor1
ciscoasa(config-pmap)# class my-ips-class2
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor2
ciscoasa(config-pmap-c)# service-policy my-ips-policy interface outside
```

Feature History for the ASA IPS module

Table 31-2 lists each feature change and the platform release in which it was implemented.

Table 31-2 Feature History for the ASA IPS module

Feature Name	Platform Releases	Feature Information
AIP SSM	7.0(1)	We introduced support for the AIP SSM for the ASA 5510, 5520, and 5540. The following command was introduced: **ips**.
Virtual sensors (ASA 5510 and higher)	8.0(2)	Virtual sensor support was introduced. Virtual sensors let you configure multiple security policies on the ASA IPS module. The following command was introduced: **allocate-ips**.
AIP SSC for the ASA 5505	8.2(1)	We introduced support for the AIP SSC for the ASA 5505. The following commands were introduced: **allow-ssc-mgmt**, **hw-module module ip**, and **hw-module module allow-ip**.
Support for the ASA IPS SSP-10, -20, -40, and -60 for the ASA 5585-X	8.2(5)/ 8.4(2)	We introduced support for the ASA IPS SSP-10, -20, -40, and -60 for the ASA 5585-X. You can only install the ASA IPS SSP with a matching-level SSP; for example, SSP-10 and ASA IPS SSP-10. **Note** The ASA 5585-X is not supported in Version 8.3.

Table 31-2 Feature History for the ASA IPS module (continued)

Feature Name	Platform Releases	Feature Information
Support for Dual SSPs for SSP-40 and SSP-60	8.4(2)	For SSP-40 and SSP-60, you can use two SSPs of the same level in the same chassis. Mixed-level SSPs are not supported (for example, an SSP-40 with an SSP-60 is not supported). Each SSP acts as an independent device, with separate configurations and management. You can use the two SSPs as a failover pair if desired. **Note** When using two SSPs in the chassis, VPN is not supported; note, however, that VPN has not been disabled. We modified the following commands: **show module**, **show inventory**, **show environment**.
Support for the ASA IPS SSP for the ASA 5512-X through ASA 5555-X	8.6(1)	We introduced support for the ASA IPS SSP software module for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X. We introduced or modified the following commands: **session**, **show module**, **sw-module**.