Configuring the ASA IPS Module

This chapter describes how to configure the ASA IPS module. The ASA IPS module might be a physical 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

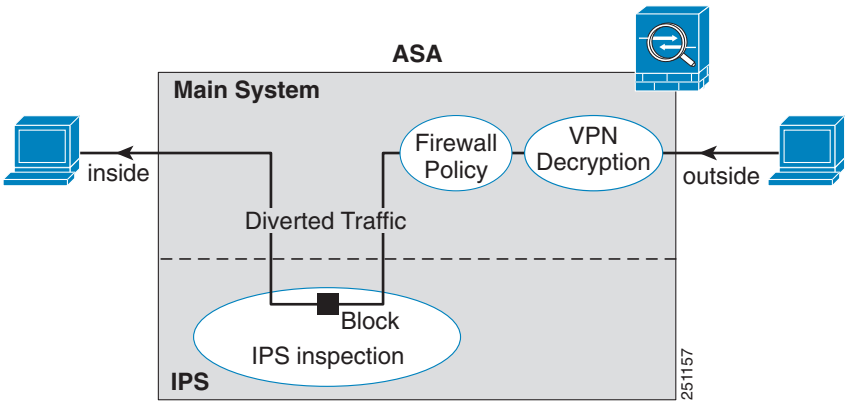
The ASA IPS module runs a separate application from the ASA. The ASA IPS module might include an external management interface so you can connect to the ASA IPS module directly; if it does not have a management interface, you can connect to the ASA IPS module through the ASA interface. The ASA IPS SSP 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 81-3 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 81-1 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 81-1 ASA IPS module Traffic Flow in the ASA: Inline Mode

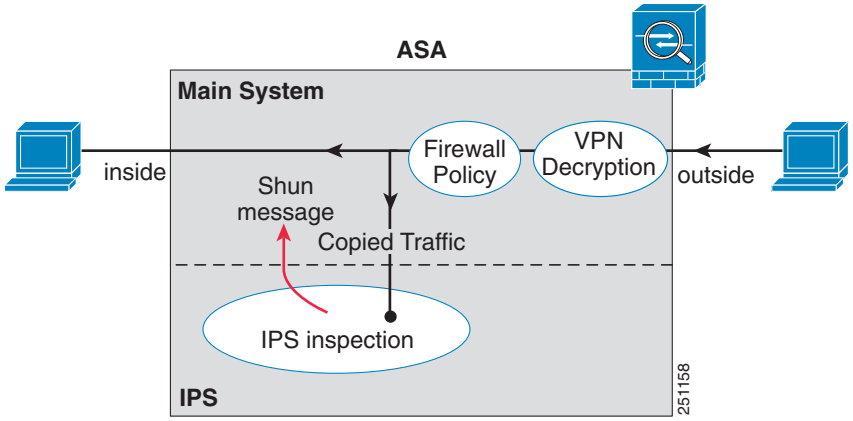


Operating Modes

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 81-1). 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 81-2 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 81-2 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 81-3 shows one security context paired with one virtual sensor (in inline mode), while two security contexts share the same virtual sensor.

Figure 81-3 Security Contexts and Virtual Sensors

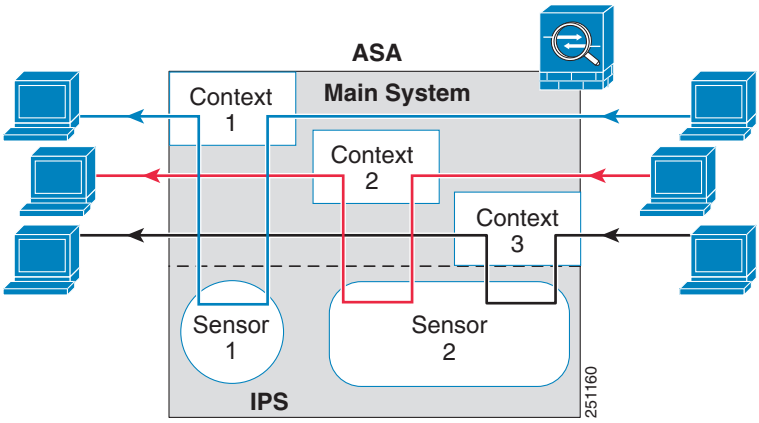
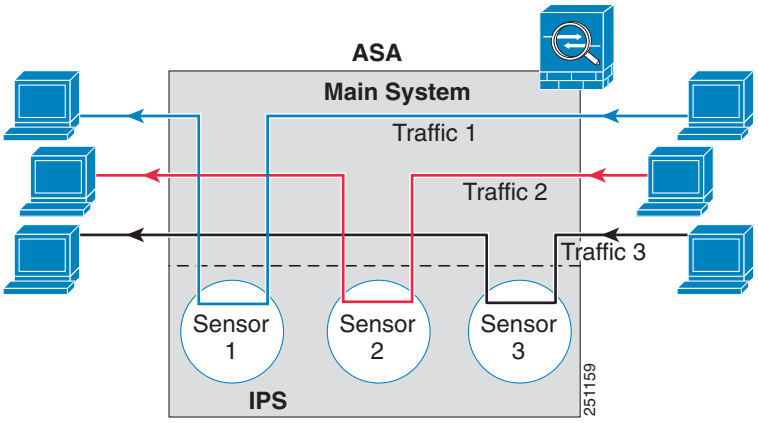


Figure 81-4 shows a single mode ASA paired with multiple virtual sensors (in inline mode); each defined traffic flow goes to a different sensor.

Figure 81-4 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 (May Be Required)" section on page 81-11.
- 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.

The ASA IPS module requires a separate Cisco Services for IPS license in order to support signature updates. All other updates are available without a 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 81-1 lists the default settings for the ASA IPS module.

Table 81-1 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 81-8.

Step 2 Session to the module. Access the IPS CLI over the backplane. For ASDM users, you may need to session to the module to boot the IPS software if it is not running. See the "Sessioning to the Module from the ASA (May Be Required)" section on page 81-11.

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 81-12.

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 81-13.
- (ASA 5505) Configure the management VLAN and IP address for the IPS module. See the "(ASA 5505) Configuring Basic Network Settings" section on page 81-14.

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 81-15.

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 81-17.

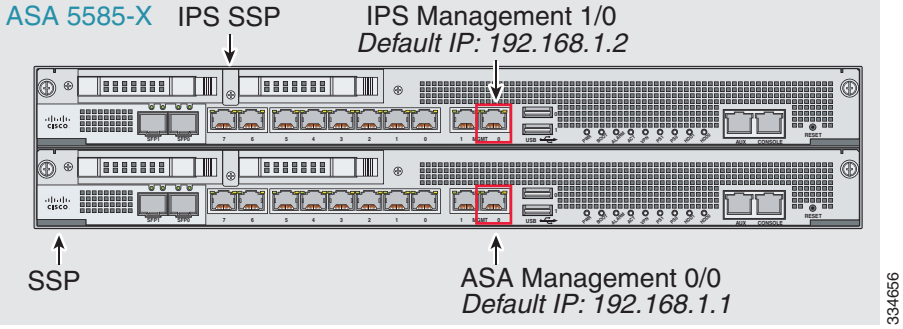
Step 7 On the ASA, identify traffic to divert to the ASA IPS module. See the "Diverting Traffic to the ASA IPS module" section on page 81-18.

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.

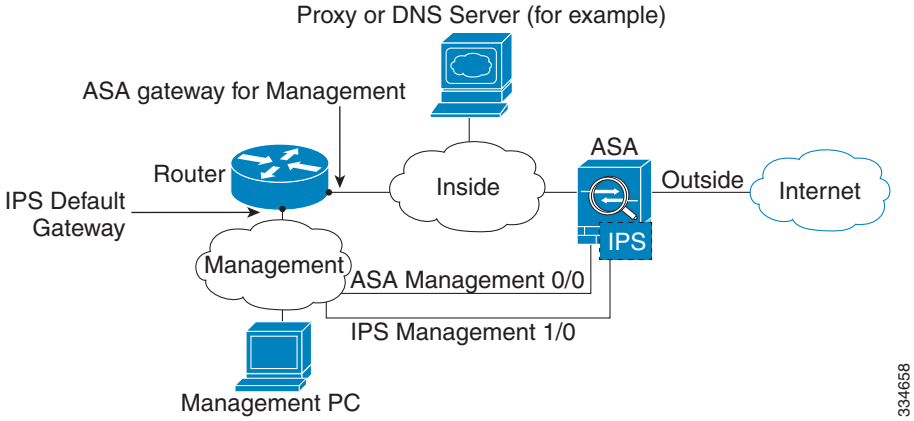
ASA 5510, ASA 5520, ASA 5540, ASA 5580, ASA 5585-X (Physical Module)

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



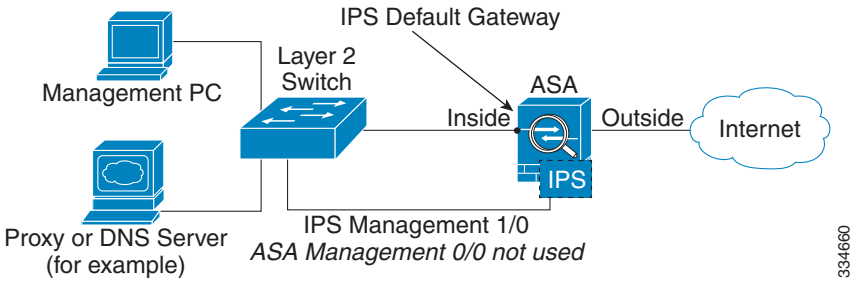
If you have an inside router

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.



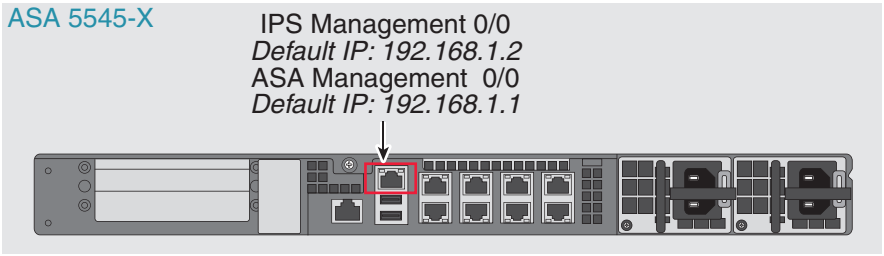
If you do not have an inside router

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.



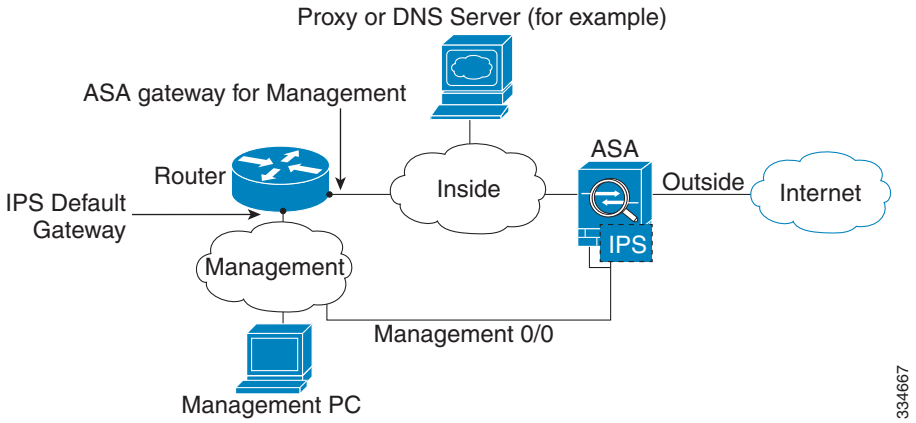
ASA 5512-X through ASA 5555-X (Software Module)

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



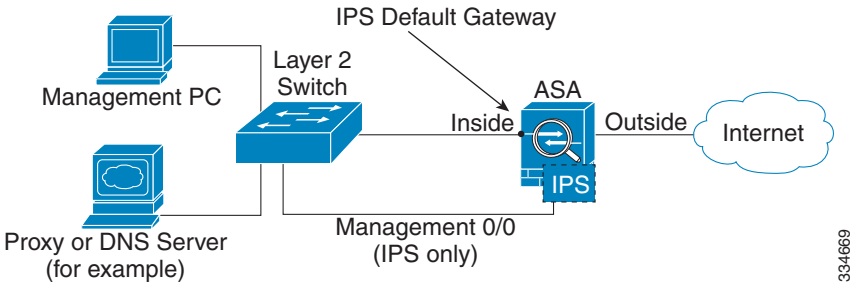
If you have an inside router

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

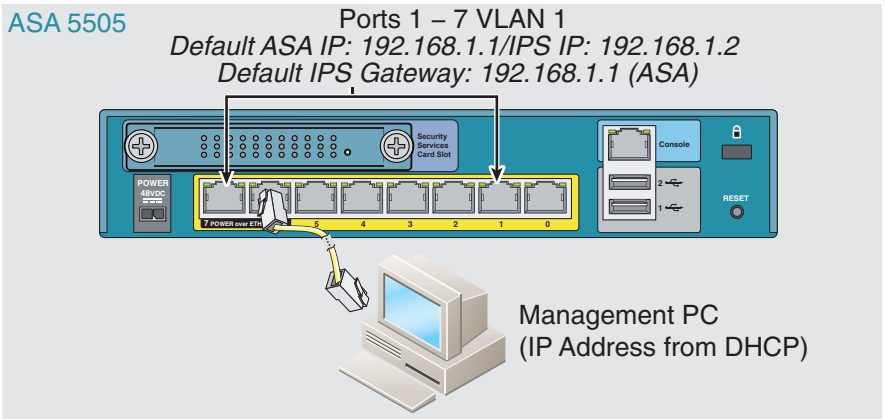
If you have only one inside network, then you cannot also have a separate management network. In this case, you can manage the ASA from the inside interface instead of the Management 0/0 interface. If you remove the ASA-configured name from the Management 0/0 interface, you can still configure the IPS 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 81-13.
- (ASA 5505) Configure management interface settings. See the "(ASA 5505) Configuring Basic Network Settings" section on page 81-14.

Sessioning to the Module from the ASA (May Be Required)

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.

You may need to access the CLI if you are using multiple context mode and you need to set basic network settings using the CLI, or for troubleshooting.

Detailed Steps

Command	Purpose

Telnet session.
 	
For a physical module (for example, the ASA 5585-X):
session 1
 	
For a software module (for example, the ASA 5545-X):
session ips
 	
Example:
`hostname# 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:
`hostname# 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 see the IPS Basic COnfiguration screen when you run the Startup Wizard (see the "Configuring Basic IPS Module Network Settings" section on page 81-12).

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, choose **Tools > File Management**.

  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 your computer. 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

  Choose **Tools > File Management**, then choose **File Transfer > Between Local PC and Flash** to upload the new image to disk0. Note the filename; you will need this filename later in the procedure.

Step 2 Choose **Tools > Command Line Interface**.

Step 3 To set the IPS module software location in disk0, enter the following command and then click **Send**:

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

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

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

Step 4 To install and load the IPS module software, enter the following command and then click **Send**:

```
sw-module module ips recover boot
```

Step 5 To check the progress of the image transfer and module restart process, enter the following command and then click **Send**:

```
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

In single context mode, you can use the Startup Wizard in ASDM to configure basic IPS network configuration. These settings are saved to the IPS configuration, not the ASA configuration.

In multiple context mode, 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 do not see the IPS Basic Configuration screen in your wizard, then the IPS module is not running. See the "(ASA 5512-X through ASA 5555-X) Booting the Software Module" section on page 81-12, and then repeat this procedure after you install the module.

Detailed Steps—Single Mode

Step 1 Choose **Wizards > Startup Wizard**.

Step 2 Click **Next** to advance through the initial screens until you reach the IPS Basic Configuration screen.

Step 3 In the Network Settings area, configure the following:

- IP Address—The management IP address. By default, the address is 192.168.1.2.
- Subnet Mask—The subnet mask for the management IP address.
- Gateway—The IP address of the upstream router. The IP address of the next hop router. See the "Connecting the ASA IPS Management Interface" section on page 81-8 to understand the requirements for your network. The default setting of the ASA management IP address will not work.
- HTTP Proxy Server—(Optional) The HTTP proxy server address. You can use a proxy server to download global correlation updates and other information instead of downloading over the Internet.
- HTTP Proxy Port—(Optional) The HTTP proxy server port.
- DNS Primary—(Optional) The primary DNS server address. If you are using a DNS server, you must configure at least one DNS server and it must be reachable for global correlation updates to be successful.

  For global correlation to function, you must have either a DNS server or an HTTP proxy server configured at all times. DNS resolution is supported only for accessing the global correlation update server.

Step 4 In the Management Access List area, enter an IP address and subnet mask for any hosts that are allowed to access the IPS management interface, and click **Add**. You can add multiple IP addresses.

Step 5 In the Cisco Account Password area, set the password for the username **cisco** and confirm it. The username **cisco** and this password are used for Telnet sessions from hosts specified by the management access list and when accessing the IPS module from ASDM (Configuration > IPS). By default, the password is **cisco**.

Step 6 In the Network Participation area, which you use to have the IPS module participate in SensorBase data sharing, click **Full**, **Partial**, or **Off**.

Detailed Steps—Multiple Mode Using the CLI

	Command	Purpose
Step 1	Session to the IPS module according to the "Sessioning to the Module from the ASA (May Be Required)" section on page 81-11.	

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 81-8 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 16, "Starting Interface Configuration (ASA 5505)." 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

Step 1 In ASDM, choose **Configuration > Device Setup > SSC Setup**.

Note The following settings are written to the ASA IPS module application configuration, not the ASA configuration.

Step 2 In the Management Interface area, set the following:

a. Choose the Interface VLAN from the drop-down list.

This setting allows you to manage the ASA IPS module using this VLAN.

b. Enter the IPS management IP address. 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. By default, the address is 192.168.1.2

c. Choose the subnet mask from the drop-down list.

d. Enter the default gateway IP address.

Set the gateway to be the ASA IP address for the management VLAN. By default, this IP address is 192.168.1.1.

Step 3 In the Management Access List area, enter the following:

a. Enter the IP address for the management host network.

b. Choose the subnet mask from the drop-down list.

c. Click **Add** to add these settings to the Allowed Hosts/Networks list.

Step 4 In the IPS Password area, do the following:

a. Enter the current password. The default password is **cisco**.

b. Enter the new password, and confirm the change.

Step 5 Click **Apply** to save the settings to the running configuration.

Step 6 To launch the IPS Startup Wizard, click the **Configure the IPS SSC module** link.

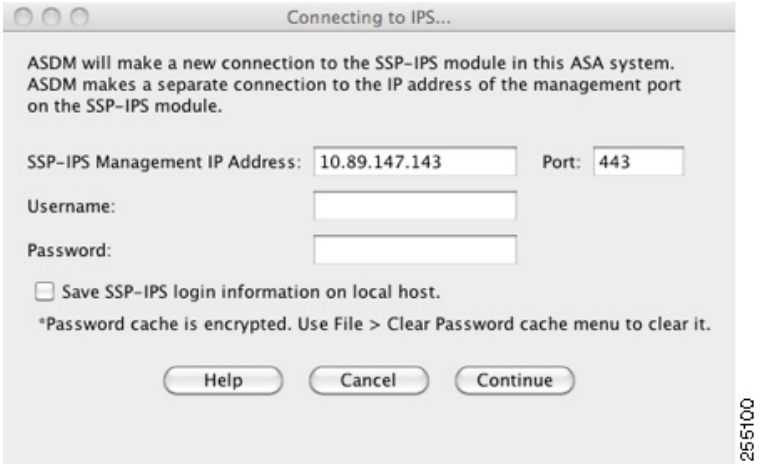
Configuring the Security Policy on the ASA IPS Module

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

Detailed Steps

Step 1 Connect to ASDM using the *ASA* management IP address. See the "Starting ASDM" section on page 3-13.

Step 2 To access the IPS Device Manager (IDM) from ASDM, click **Configuration > IPS**.



Step 3 Enter the IP address, username and password that you set in the "Configuring Basic IPS Module Network Settings" section on page 81-12, as well as the port. The default IP address and port is 192.168.1.2:443. The default username and password is **cisco** and **cisco**.

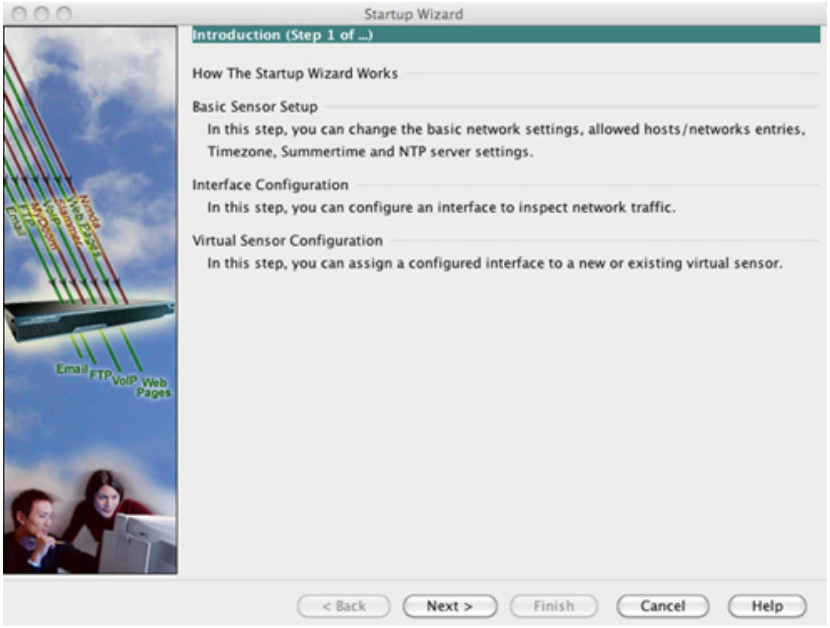
If the password to access IDM is lost, you can reset the password using ASDM. See the "Resetting the Password" section on page 81-22, for more information.

Step 4 To save the login information on your local PC, check the **Save IPS login information on local host** check box.

Step 5 Click **Continue**.

The Startup Wizard pane appears.

Step 6 Click **Launch Startup Wizard**. Complete the screens as prompted. For more information, see the IDM online help.



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

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 81-17.
- For the ASA in single context mode, see the "Diverting Traffic to the ASA IPS module" section on page 81-18.

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 9-15.

Detailed Steps

Step 1 In the ASDM Device List pane, double-click **System** under the active device IP address.

Step 2 On the Context Management > Security Contexts pane, choose a context that you want to configure, and click **Edit**.

The Edit Context dialog box appears. For more information about configuring contexts, see the "Configuring Multiple Contexts" section on page 9-15.

Step 3 In the IPS Sensor Allocation area, click **Add**.

The IPS Sensor Selection dialog box appears.

Step 4 From the Sensor Name drop-down list, choose a sensor name from those configured on the ASA IPS module.

Step 5 (Optional) To assign a mapped name to the sensor, enter a value in the Mapped Sensor Name field.

This sensor name 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.

Step 6 Click **OK** to return to the Edit Context dialog box.

Step 7 (Optional) To set one sensor as the default sensor for this context, from the Default Sensor drop-down list, choose a sensor name.

If you do not specify a sensor name when you configure IPS within the context configuration, the context uses this default sensor. You can only configure one default sensor per context. 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 on the ASA IPS module.

Step 8 Repeat this procedure for each security context.

Step 9 Change to each context to configure the IPS security policy as described in "Diverting Traffic to the ASA IPS module" section on page 81-18.

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 81-18.

Diverting Traffic to the ASA IPS module

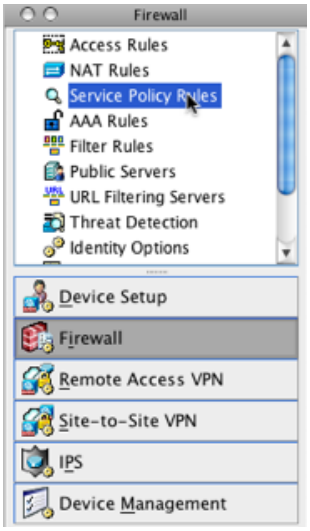
This section identifies traffic to divert from the ASA to the ASA IPS module.

Prerequisites

In multiple context mode, perform these steps in each context execution space. To change to a context, in the Configuration > Device List pane, double-click the context name under the active device IP address.

Detailed Steps

Step 1 Choose **Configuration > Firewall > Service Policy Rules**.

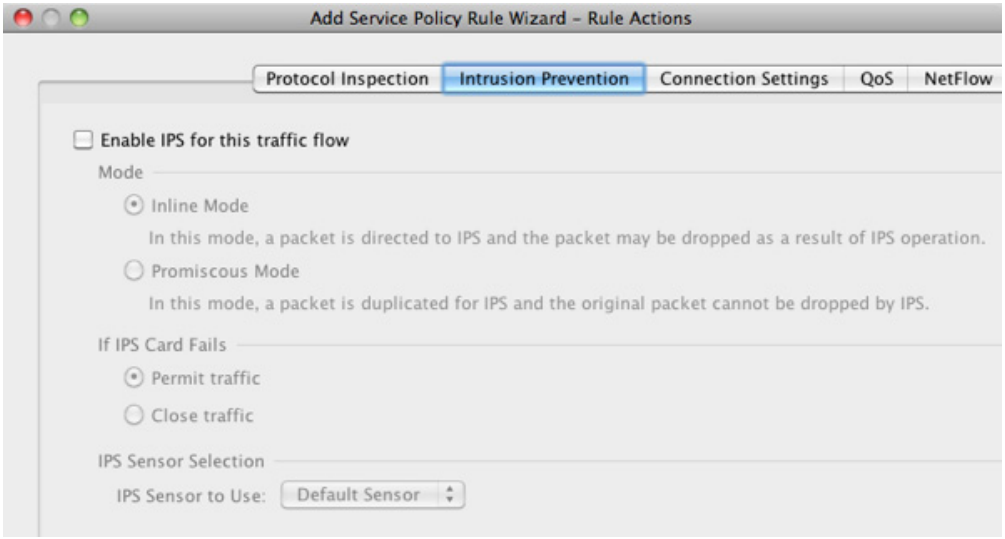


Step 2 Choose **Add > Add Service Policy Rule**. The Add Service Policy Rule Wizard - Service Policy dialog box appears.

Step 3 Complete the Service Policy dialog box, and then the Traffic Classification Criteria dialog box as desired. See the ASDM online help for more information about these screens.

Step 4 Click **Next** to show the Add Service Policy Rule Wizard - Rule Actions dialog box.

Step 5 Click the **Intrusion Prevention** tab.



Step 6 Check the **Enable IPS for this traffic flow** check box.

Step 7 In the Mode area, click **Inline Mode** or **Promiscuous Mode**. See the "Operating Modes" section on page 81-3 for more information.

Step 8 In the If IPS Card Fails area, click **Permit traffic** or **Close traffic**. The Close traffic option sets the ASA to block all traffic if the ASA IPS module is unavailable. The Permit traffic option sets the ASA to allow all traffic through, uninspected, if the ASA IPS module is unavailable. For information about the IPS Sensor Selection area, see the ASDM online help.

Step 9 (ASA 5510 and higher) From the IPS Sensor to use drop-down list, choose a virtual sensor name.

If you use virtual sensors, you can specify a sensor name using this option. 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 81-17). 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.

Step 10 Click **OK** and then **Apply**.

Step 11 Repeat this procedure to configure additional traffic flows as desired.

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, page 81-20
- Shutting Down the Module, page 81-22

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 physical module), or from the local disk (software module).

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

Prerequisites

- Physical 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 physical 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:
	`hostname# 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 physical 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 physical module: **hw-module module 1 recover boot** For a software module: **sw-module module ips recover boot** **Example:** `hostname# hw-module module 1 recover boot`	Installs and boots the IPS module software.
Step 3	For a physical module: **show module 1 details** For a software module: **show module ips details** **Example:** `hostname# 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 physical 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:** `hostname# 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

sw-module module ips uninstall
 	
Example:
`hostname# 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.

Resetting the Password

You can reset the module password to the default. 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.

If you cannot connect to ASDM with the new password, restart ASDM and try to log in again. If you defined a new password and still have an existing password in ASDM that is different from the new password, clear the password cache by choosing **File > Clear ASDM Password Cache**, then restart ASDM and try to log in again.

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

Detailed Steps

Step 1 From the ASDM menu bar, choose **Tools >** *module* **Password Reset**.

The Password Reset confirmation dialog box appears.

Step 2 Click **OK** to reset the password to the default.

A dialog box displays the success or failure of the password reset.

Step 3 Click **Close** to close the dialog box.

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 physical 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:** `hostname# hw-module module 1 reload`	Reloads the module software.
For a physical module: **hw-module module 1 reset** For a software module: **sw-module module ips reset** **Example:** `hostname# hw-module module 1 reset`	Performs a reset, and then reloads the module.

Monitoring the ASA IPS module

See the "Intrusion Prevention Tab" section on page 4-28.

Feature History for the ASA IPS module

Table 81-2 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 81-2 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 screen was introduced: Configuration > Firewall > Service Policy Rules > Add/Edit Service Policy Rule > Intrusion Prevention.
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 screen was modified: Context Management > Security Contexts > Edit Context.
AIP SSC for the ASA 5505	8.2(1)	We introduced support for the AIP SSC for the ASA 5505. The following screen was introduced: Configuration > Device Setup > SSC Setup.
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 81-2 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 did not modify any screens.
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 did not modify any screens.