



CHAPTER 28

Configuring IPS

This chapter describes how to configure the adaptive security appliance to support an AIP SSM that is installed in the security appliance.



Note

The Cisco PIX 500 series security appliances do not support SSMs.

This chapter includes the following sections:

- [AIP SSM Overview, page 28-1](#)
- [Accessing IDM from ASDM, page 28-5](#)
- [Configuring the AIP SSM Security Policy in IDM, page 28-5](#)
- [Assigning Virtual Sensors to Security Contexts, page 28-5](#)
- [Diverting Traffic to the AIP SSM, page 28-6](#)
- [Resetting the AIP SSM Password, page 28-8](#)

AIP SSM Overview

You can install the AIP SSM into an ASA 5500 series adaptive security appliance. The AIP SSM 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 AIP SSM Works with the Adaptive Security Appliance, page 28-2](#)
- [Operating Modes, page 28-2](#)
- [Using Virtual Sensors, page 28-3](#)
- [AIP SSM Procedure Overview, page 28-4](#)

How the AIP SSM Works with the Adaptive Security Appliance

The AIP SSM runs a separate application from the adaptive security appliance. It is, however, integrated into the adaptive security appliance traffic flow. The AIP SSM does not contain any external interfaces itself, other than a management interface. When you identify traffic for IPS inspection on the adaptive security appliance, traffic flows through the adaptive security appliance and the AIP SSM in the following way:

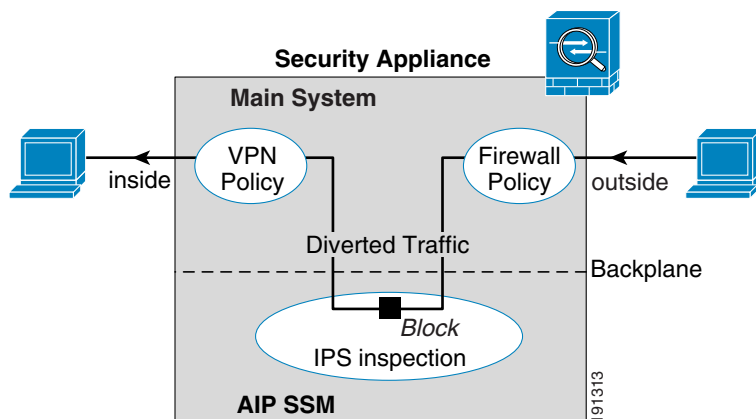
1. Traffic enters the adaptive security appliance.
2. Firewall policies are applied.
3. Traffic is sent to the AIP SSM over the backplane.

See the “[Operating Modes](#)” section on page 28-2 for information about only sending a copy of the traffic to the AIP SSM.

4. The AIP SSM applies its security policy to the traffic, and takes appropriate actions.
5. Valid traffic is sent back to the adaptive security appliance over the backplane; the AIP SSM might block some traffic according to its security policy, and that traffic is not passed on.
6. VPN policies are applied (if configured).
7. Traffic exits the adaptive security appliance.

Figure 28-1 shows the traffic flow when running the AIP SSM in inline mode. In this example, the AIP SSM automatically blocks traffic that it identified as an attack. All other traffic is forwarded through the security appliance.

Figure 28-1 AIP SSM Traffic Flow in the Adaptive Security Appliance: Inline Mode



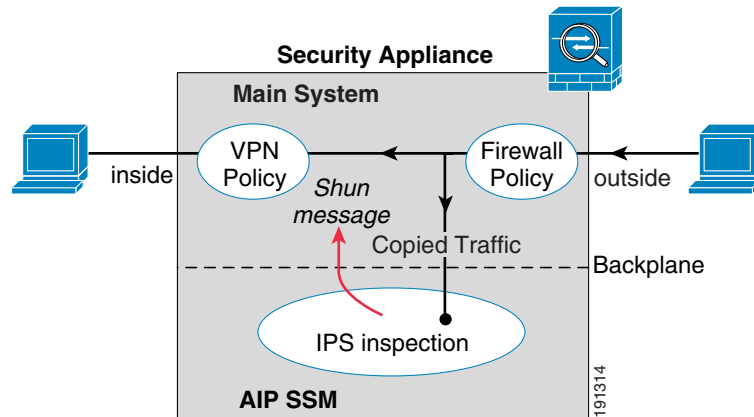
Operating Modes

You can send traffic to the AIP SSM using one of the following modes:

- **Inline mode**—This mode places the AIP SSM directly in the traffic flow (see Figure 28-1). No traffic that you identified for IPS inspection can continue through the adaptive security appliance without first passing through, and being inspected by, the AIP SSM. This mode is the most secure because every packet that you identify for inspection is analyzed before being allowed through. Also, the AIP SSM 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 AIP SSM. This mode is less secure, but has little impact on traffic throughput. Unlike the inline mode, in promiscuous mode the AIP SSM can only block traffic by instructing the adaptive security appliance to shun the traffic or by resetting a connection on the adaptive security appliance. Also, while the AIP SSM is analyzing the traffic, a small amount of traffic might pass through the adaptive security appliance before the AIP SSM can shun it. [Figure 28-2](#) shows the AIP SSM in promiscuous mode. In this example, the AIP SSM sends a shun message to the security appliance for traffic it identified as a threat.

Figure 28-2 AIP SSM Traffic Flow in the Adaptive Security Appliance: Promiscuous Mode



Using Virtual Sensors

The AIP SSM running IPS software Version 6.0 and later can run multiple virtual sensors, which means you can configure multiple security policies on the AIP SSM. You can assign each context or single mode security appliance 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 28-3](#) shows one security context paired with one virtual sensor (in inline mode), while two security contexts share the same virtual sensor.

Figure 28-3 Security Contexts and Virtual Sensors

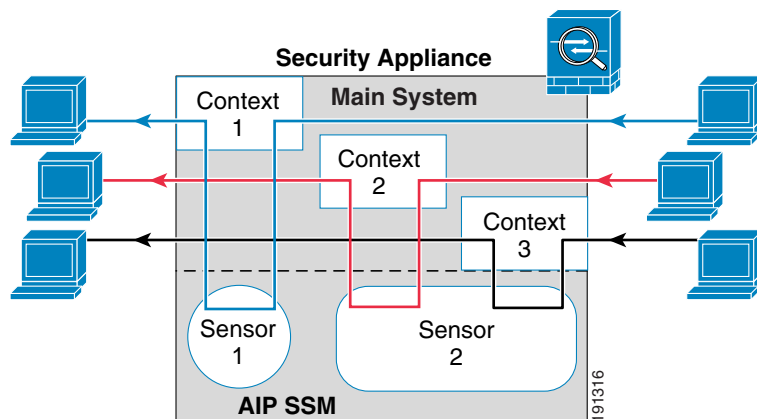
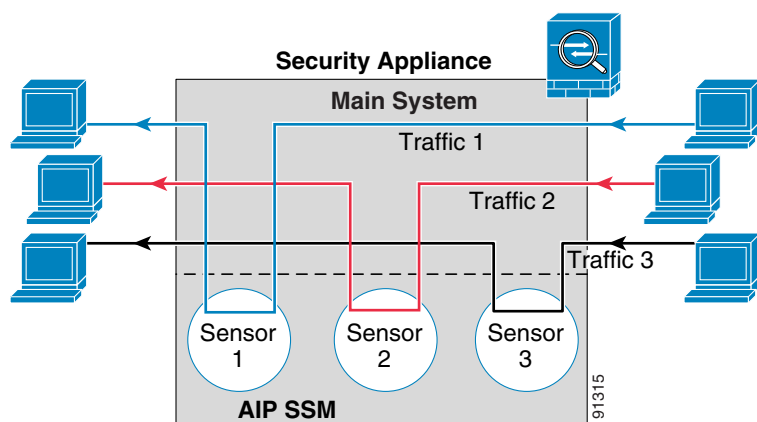


Figure 28-4 shows a single mode security appliance paired with multiple virtual sensors (in inline mode); each defined traffic flow goes to a different sensor.

Figure 28-4 Single Mode Security Appliance with Multiple Virtual Sensors



AIP SSM Procedure Overview

Configuring the AIP SSM is a process that includes configuration of the AIP SSM and then configuration of the ASA 5500 series adaptive security appliance:

1. From ASDM, launch IDM. See the [“Accessing IDM from ASDM”](#) section on page 28-5. ASDM uses IDM to configure the AIP SSM.
2. In IDM, configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. Configure the inspection and protection policy for each virtual sensor if you want to run the AIP SSM in multiple sensor mode. See the [“Configuring the AIP SSM Security Policy in IDM”](#) section on page 28-5.
3. Using ASDM on the ASA 5500 series adaptive security appliance 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 Security Contexts”](#) section on page 28-5.

- Using ASDM on the ASA 5500 series adaptive security appliance, identify traffic to divert to the AIP SSM. See the “[Diverting Traffic to the AIP SSM](#)” section on page 28-6.

Accessing IDM from ASDM

ASDM uses IDM to configure the AIP SSM. If the AIP SSM is running IPS Version 6.0 or later, ASDM retrieves IDM from the AIP SSM and displays it as part of the ASDM interface. For earlier versions of the IPS software, IDM launches in a separate browser window.

To access IDM from ASDM, click **Configuration > IPS**.

You are asked for the IP address or hostname of the AIP SSM.

- If the AIP SSM is running IPS Version 6.0 or later, ASDM retrieves IDM from the AIP SSM and displays it as part of the ASDM interface. Enter the AIP SSM password and click **OK**.

The IDM panes appear in the ASDM window.

- If the AIP SSM is running an earlier version of IPS software, ASDM displays a link to IDM. Click the link to launch IDM in a new browser window. You need to provide a username and password to access IDM.

If the password to access IDM is lost, you can reset the password using ASDM. See the “[Resetting the AIP SSM Password](#)” section on page 28-8, for more information.

Configuring the AIP SSM Security Policy in IDM

On the AIP SSM, configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. If you configure virtual sensors in IPS Version 6.0 or above, you identify one of the sensors as the default. If the ASA 5500 series adaptive security appliance does not specify a virtual sensor name in its configuration, the default sensor is used.

Because the IPS software that runs on the AIP SSM is beyond the scope of this document, detailed configuration information is available in the IDM online help. The IDM online help is available from the IDM panes displayed in ASDM. Additionally, you can see the IDM and IPS documentation on Cisco.com at the following location:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_installation_and_configuration_guides_list.html

Assigning Virtual Sensors to Security Contexts

If the security appliance 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 AIP SSM, 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 AIP SSM 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.

To assign one or more sensors to a security context, perform the following 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 Security Contexts” section on page 10-16](#).
- 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 AIP SSM.
- 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 AIP SSM.
- 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 AIP SSM” section on page 28-6](#).
-

Diverting Traffic to the AIP SSM

To identify traffic to divert from the adaptive security appliance to the AIP SSM, perform the following steps. In multiple context mode, perform these steps in each context execution space.

This feature is enabled using Service Policy rules. See [Chapter 22, “Configuring Service Policy Rules,”](#) for detailed information about creating a service policy.

-
- Step 1** In the ASDM Device List pane, double-click the context name under the active device *IP address* > Contexts.
- Step 2** Click **Configuration > Firewall > Service Policy Rules**.
- Step 3** You can edit an existing rule or create a new one:
- For an existing rule, choose the rule and click **Edit**.
The Edit Service Policy Rule dialog box appears.
 - For a new rule, choose **Add > Add Service Policy Rule**.

The Add Service Policy Rule Wizard - Service Policy dialog box appears. Complete the Service Policy and Traffic Classification Criteria dialog boxes. See the [“Adding a Service Policy Rule for Through Traffic”](#) section on page 22-6 for more information. Click **Next** to show the Add Service Policy Rule Wizard - Rule Actions dialog box.

Step 4 Click the **Intrusion Prevention** tab.

You can also set other feature actions for the same traffic using the other tabs.

Step 5 Check the **Enable IPS for this traffic flow** check box.

Step 6 In the Mode area, click **Inline Mode** or **Promiscuous Mode**.

See the [“Operating Modes”](#) section on page 28-2 for more details.

Step 7 In the If IPS Card Fails area, click **Permit traffic** or **Close traffic**.

The Close traffic option sets the adaptive security appliance to block all traffic if the AIP SSM is unavailable.

The Permit traffic option sets the adaptive security appliance to allow all traffic through, uninspected, if the AIP SSM is unavailable.

Step 8 (Optional) From the IPS Sensor to use drop-down list, choose a virtual sensor name.

If you use virtual sensors on the AIP SSM, you can specify a sensor name using this option. If you use multiple context mode on the security appliance, you can only specify sensors that you assigned to the context (see the [“Assigning Virtual Sensors to Security Contexts”](#) section on page 28-5). 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 AIP SSM.

Step 9 Click **OK**.

Intrusion Prevention Tab Field Descriptions

Fields

- Enable IPS for this traffic flow—Enables or disables intrusion prevention for this traffic flow. When this check box is checked, the other parameters on this window become active.
- Mode—Configures the operating mode for intrusion prevention. See the [“Operating Modes”](#) section on page 28-2 for more information.
 - Inline Mode—Selects Inline Mode, in which a packet is directed to IPS. The packet might be dropped as a result of the IPS operation.
 - Promiscuous Mode—Selects Promiscuous Mode, in which IPS operates on a duplicate of the original packet. The original packet cannot be dropped.
- If IPS card fails—Configures the action to take if the AIP SSM becomes inoperable.
 - Permit traffic—Permit traffic if the AIP SSM fails
 - Close traffic—Block traffic if the AIP SSM fails.
- IPS Sensor Selection—Selects the virtual sensor to use for this traffic flow. See the [“Using Virtual Sensors”](#) section on page 28-3 for more information.
 - IPS Sensor to Use—Sets a virtual sensor name. If you use virtual sensors on the AIP SSM, you can specify a sensor name using this option. If you use multiple context mode on the security appliance, you can only specify sensors that you assigned to the context (see the [“Assigning](#)

[Virtual Sensors to Security Contexts](#)” section on page 28-5). 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 AIP SSM.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

Resetting the AIP SSM Password

You can use ASDM to reset the AIP SSM password to the default if the AIP SSM is running IPS Version 6.0 or later. The default password is “cisco” (without the quotation marks). After resetting the password, you should change it to a unique value using IDM. See the [“Accessing IDM from ASDM” section on page 28-5](#) for information about accessing IDM from ASDM.

Resetting the AIP SSM password causes the AIP SSM to reboot. IPS services are not available while the AIP SSM is rebooting.

To reset the AIP SSM password to the default, perform the following steps:

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



Note This option does not appear in the menu if an SSM is not installed. This option appears as CSC Password Reset if a CSC SSM is installed.

The IPS Password Reset confirmation dialog box appears.

- Step 2** Click **OK** to reset the AIP SSM password to the default.

A dialog box displays the success or failure of the password reset. If the password was not reset, make sure you are using Version 7.2(2) or later of the platform software on the adaptive security appliance and IPS Version 6.0 or later on the AIP SSM.

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