



CHAPTER 30

Configuring the IPS Application on the AIP SSM and SSC

This chapter describes how to configure the IPS application that runs on an AIP SSM or an AIP SSC.



Note

The SSC is supported on the ASA 5505. See the [“SSM and SSC Support Per Model”](#) section on page 3-2 for more information about which models support SSMs.

This chapter includes the following sections:

- [Information About the AIP SSM and SSC, page 30-1](#)
- [Licensing Requirements for the AIP SSM/SSC, page 30-4](#)
- [Guidelines and Limitations, page 30-5](#)
- [Configuring the AIP SSM/SSC, page 30-5](#)
- [Feature History for the AIP SSM/SSC, page 30-10](#)

Information About the AIP SSM and SSC

You can install the AIP SSM/SSC into an ASA 5500 series adaptive security appliance. The AIP SSM/SSC 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/SSC Works with the Adaptive Security Appliance, page 30-2](#)
- [Operating Modes, page 30-2](#)
- [Using Virtual Sensors \(AIP SSM Only\), page 30-3](#)
- [Differences Between the AIP SSM and the AIP SSC, page 30-4](#)

How the AIP SSM/SSC Works with the Adaptive Security Appliance

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

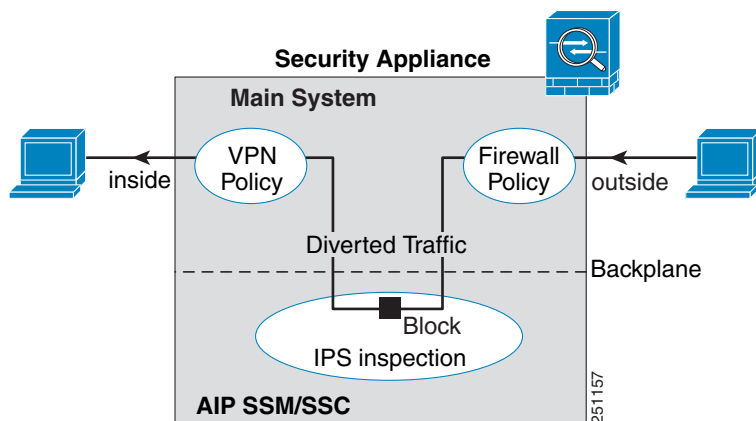
1. Traffic enters the security appliance.
2. Firewall policies are applied.
3. Traffic is sent to the AIP SSM/SSC over the backplane.

See the “[Operating Modes](#)” section on page 30-2 for information about only sending a copy of the traffic to the AIP SSM/SSC.

4. The AIP SSM/SSC 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 in inline mode; the AIP SSM/SSC 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 30-1 shows the traffic flow when running the AIP SSM/SSC in inline mode. In this example, the AIP SSM/SSC automatically blocks traffic that it identified as an attack. All other traffic is forwarded through the security appliance.

Figure 30-1 AIP SSM/SSC Traffic Flow in the Adaptive Security Appliance: Inline Mode



Operating Modes

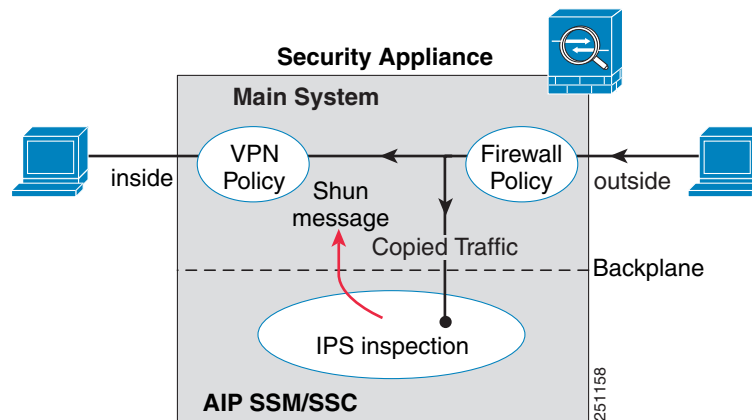
You can send traffic to the AIP SSM/SSC using one of the following modes:

- Inline mode—This mode places the AIP SSM/SSC directly in the traffic flow [Figure 30-1](#). 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/SSC. This mode is the most secure

because every packet that you identify for inspection is analyzed before being allowed through. Also, the AIP SSM/SSC 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/SSC. This mode is less secure, but has little impact on traffic throughput. Unlike the inline mode, in promiscuous mode the AIP SSM/SSC 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/SSC is analyzing the traffic, a small amount of traffic might pass through the adaptive security appliance before the AIP SSM/SSC can shun it.
- [Figure 30-2](#) shows the AIP SSM/SSC in promiscuous mode. In this example, the AIP SSM/SSC sends a shun message to the security appliance for traffic it identified as a threat.

Figure 30-2 AIP SSM/SSC Traffic Flow in the Adaptive Security Appliance: Promiscuous Mode



Using Virtual Sensors (AIP SSM Only)

The AIP SSM running IPS software Version 6.0 and above 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 30-3](#) shows one security context paired with one virtual sensor (in inline mode), while two security contexts share the same virtual sensor.

Figure 30-3 Security Contexts and Virtual Sensors

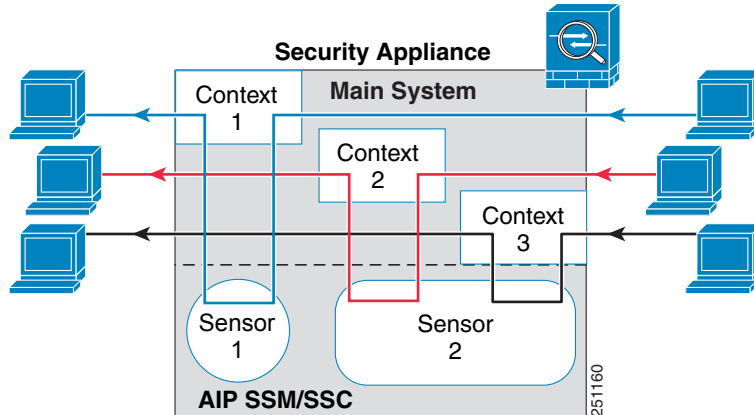
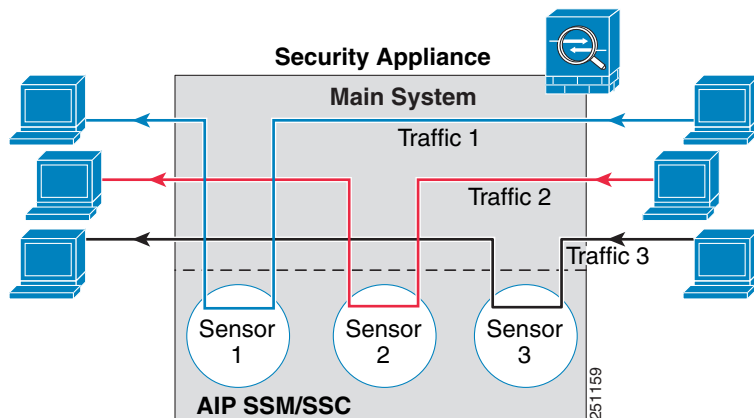


Figure 30-4 shows a single mode security appliance paired with multiple virtual sensors (in inline mode); each defined traffic flow goes to a different sensor.

Figure 30-4 Single Mode Security Appliance with Multiple Virtual Sensors



Differences Between the AIP SSM and the AIP SSC

The AIP SSM supports the higher performance requirements of the ASA 5510 and above, while the AIP SSC is designed for the small office installation of the ASA 5505 security appliance. The following features are supported on the AIP SSM, but not on the AIP SSC:

- Virtual sensors
- Anomaly detection
- Unretirement of default retired signatures

Licensing Requirements for the AIP SSM/SSC

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

The IPS application on the AIP SSM/SSC 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 adaptive security appliance 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

- The SSC is supported on the ASA 5505 only. See the [“Supported Platforms and SSMs” section on page 2-2](#) for more information about which models support SSMs.
- The ASA 5505 adaptive security appliance does not support multiple context mode, so multiple context features, such as virtual sensors, are not supported on the AIP SSC.

Configuring the AIP SSM/SSC

This section describes how to configure IPS for the AIP SSM and AIP SSC, and includes the following topics:

- [AIP SSM/SSC Task Overview, page 30-6](#)
- [Configuring the Security Policy on the AIP SSM/SSC, page 30-6](#)
- [Assigning Virtual Sensors to Security Contexts \(AIP SSM Only\), page 30-7](#)
- [Diverting Traffic to the AIP SSM/SSC, page 30-8](#)
- [Resetting the AIP SSM/SSC Password, page 30-9](#)

AIP SSM/SSC Task Overview

Configuring the AIP SSM/SSC is a process that includes configuration of the IPS software on the SSM/SSC and then configuration of the ASA 5500 series adaptive security appliance. To configure the AIP SSM/SSC, perform the following steps:

-
- Step 1** From ASDM, launch IDM. ASDM uses IDM to configure the AIP SSM. In IDM, configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. For the AIP SSM only, 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 Security Policy on the AIP SSM/SSC”](#) section on page 30-6.
- Step 2** (AIP SSM only) Using ASDM on the ASA 5500 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 \(AIP SSM Only\)”](#) section on page 30-7.
- Step 3** Using ASDM on the ASA 5500, identify traffic to divert to the AIP SSM/SSC. See the [“Diverting Traffic to the AIP SSM/SSC”](#) section on page 30-8.
-

Configuring the Security Policy on the AIP SSM/SSC

ASDM uses IDM to configure the AIP SSM. This section describes how to access IDM from within ASDM.

**Note**

See also the [“Configuring the SSC Management Interface”](#) section on page 10-3 to configure the SSC management interface for ASDM access and other uses.

Detailed Steps

-
- Step 1** To access IDM from ASDM, click **Configuration > IPS**.
- Step 2** You are asked for the IP address or hostname of the AIP SSM/SSC.
- If the AIP SSM/SSC is running IPS Version 6.0 or later, ASDM retrieves IDM from the AIP SSM/SSC and displays it as part of the ASDM interface. Enter the AIP SSM/SSC password and click **OK**.
The IDM panes appear in the ASDM window.
 - For the AIP SSM only, if it 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/SSC Password”](#) section on page 30-9, for more information.
- Step 3** Configure the IPS security policy.
- For the AIP SSM only, 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/SSC is beyond the scope of this document, detailed configuration information is available in the IPS documents at the following location:

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

What to Do Next

For the security appliance in multiple context mode, see the “Assigning Virtual Sensors to Security Contexts (AIP SSM Only)” section on page 30-7.

For the security appliance in single context mode, see the “Diverting Traffic to the AIP SSM/SSC” section on page 30-8.

Assigning Virtual Sensors to Security Contexts (AIP SSM Only)

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.

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 Security Contexts” section on page 11-16.
- 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/SSC” section on page 30-8](#).
-

What to Do Next

Change to each context to configure the IPS security policy as described in [“Diverting Traffic to the AIP SSM/SSC” section on page 30-8](#).

Diverting Traffic to the AIP SSM/SSC

To identify traffic to divert from the adaptive security appliance to the AIP SSM/SSC, 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 23, “Configuring Service Policy Rules,”](#) for detailed information about creating a service policy.

To configure the IPS service policy, perform the following steps:

- 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 23-7](#) 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 30-2](#) 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/SSC is unavailable.
The Permit traffic option sets the adaptive security appliance to allow all traffic through, uninspected, if the AIP SSM/SSC is unavailable.

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

If you use virtual sensors on the AIP SSM only, 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 \(AIP SSM Only\)”](#) section on page 30-7). 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**.

Resetting the AIP SSM/SSC Password

You can use ASDM to reset the AIP SSM/SSC password to the default if the AIP SSM/SSC 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 [“AIP SSM/SSC Task Overview”](#) section on page 30-6 for information about accessing IDM from ASDM.

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

To reset the AIP SSM/SSC 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/SSC 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 IPS Version 6.0 or later on the AIP SSM/SSC.

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

Feature History for the AIP SSM/SSC

Table 30-1 lists the release history for this feature.

Table 30-1 Feature History for the AIP SSM/SSC

Feature Name	Releases	Feature Information
AIP SSM	7.0(1)	The AIP SSM was introduced. The following command was introduced: ips .
Virtual sensors	8.0(2)	Virtual sensor support was introduced. Virtual sensors let you configure multiple security policies on the AIP SSM. The following command was introduced: allocate-ips .
AIP SSC for the ASA 5505	8.2(1)	The AIP SSC was introduced. The following commands were introduced: allow-ssc-mgmt , hw-module module ip , and hw-module module allow-ip .