CHAPTER 59

Configuring the IPS Module

This chapter describes how to configure the IPS application that runs on the following module types:

- Security Services Cards (SSCs)
- Security Services Modules (SSMs)
- Security Services Processors (SSPs)

For a list of supported IPS modules per ASA model, see the *Cisco ASA 5500 Series Hardware and Software Compatibility*:

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

This chapter includes the following sections:

- Information About the IPS Module, page 59-1
- Licensing Requirements for the IPS Module, page 59-4
- Guidelines and Limitations, page 59-4
- Configuring the IPS Module, page 59-5
- Monitoring the IPS Module, page 59-10
- Configuration Examples for the IPS Module, page 59-10
- Feature History for the IPS Module, page 59-11

Information About the IPS Module

The 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 IPS Module Works with the Adaptive Security Appliance, page 59-2
- Operating Modes, page 59-2
- Using Virtual Sensors (ASA 5510 and Higher), page 59-3
- Differences Between Modules, page 59-4

How the IPS Module Works with the Adaptive Security Appliance

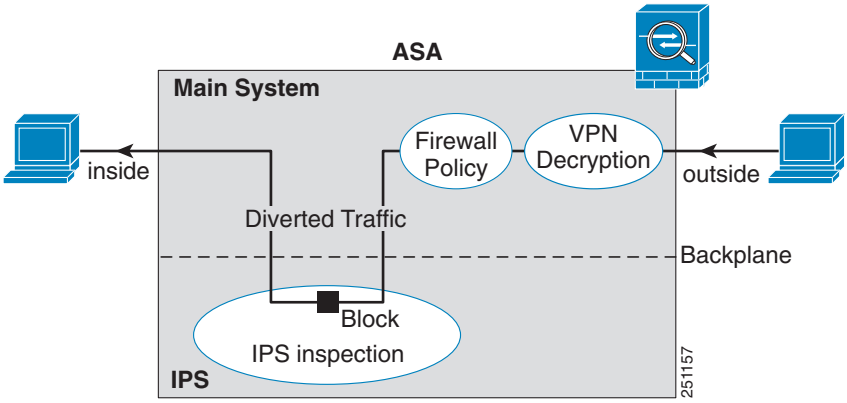
The IPS module runs a separate application from the ASA. It is, however, integrated into the ASA traffic flow. The IPS module does not contain any external interfaces itself (except for the management interface on the SSM only). When you identify traffic for IPS inspection on the ASA, traffic flows through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

1. Traffic enters the ASA.
2. Incoming VPN traffic is decrypted.
3. Firewall policies are applied.
4. Traffic is sent to the IPS module over the backplane.

   See the "Operating Modes" section on page 59-2 for information about only sending a copy of the traffic to the IPS module.
5. The IPS module applies its security policy to the traffic, and takes appropriate actions.
6. Valid traffic is sent back to the adaptive security appliance over the backplane; the 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 adaptive security appliance.

Figure 59-1 shows the traffic flow when running the IPS module in inline mode. In this example, the IPS module automatically blocks traffic that it identified as an attack. All other traffic is forwarded through the ASA.

Figure 59-1 IPS Module Traffic Flow in the Adaptive Security Appliance: Inline Mode



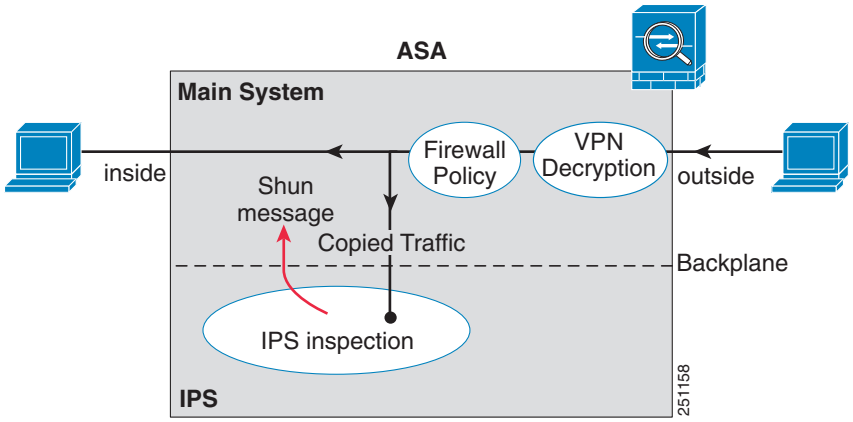
Operating Modes

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

- Inline mode—This mode places the IPS module directly in the traffic flow (see Figure 59-1). No traffic that you identified for IPS inspection can continue through the ASA without first passing through, and being inspected by, the IPS module. This mode is the most secure because every packet that you identify for inspection is analyzed before being allowed through. Also, the 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 IPS module. This mode is less secure, but has little impact on traffic throughput. Unlike the inline mode, in promiscuous mode the IPS module can only block traffic by instructing the adaptive ASA to shun the traffic or by resetting a connection on the ASA. Also, while the IPS module is analyzing the traffic, a small amount of traffic might pass through the adaptive ASA before the IPS module can shun it. Figure 59-2 shows the IPS module in promiscuous mode. In this example, the IPS module sends a shun message to the ASA for traffic it identified as a threat.

Figure 59-2 IPS Module Traffic Flow in the Adaptive Security Appliance: Promiscuous Mode



Using Virtual Sensors (ASA 5510 and Higher)

The IPS module running IPS software Version 6.0 and above can run multiple virtual sensors, which means you can configure multiple security policies on the IPS module. You can assign each 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 59-3 shows one security context paired with one virtual sensor (in inline mode), while two security contexts share the same virtual sensor.

Figure 59-3 Security Contexts and Virtual Sensors

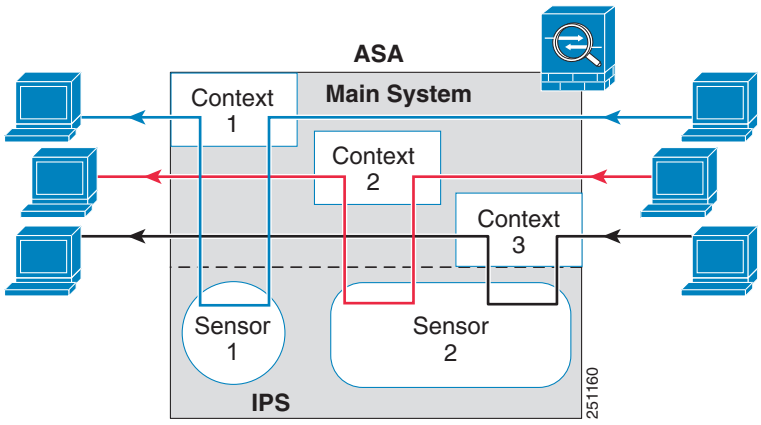
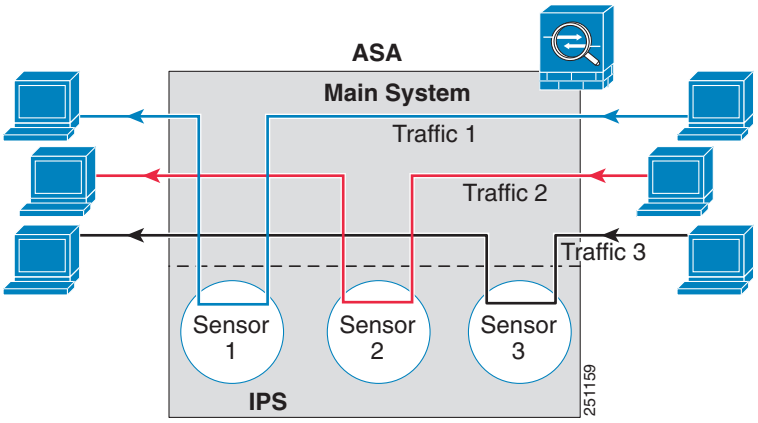


Figure 59-4 shows a single mode ASA paired with multiple virtual sensors (in inline mode); each defined traffic flow goes to a different sensor.

Figure 59-4 Single Mode Security Appliance with Multiple Virtual Sensors



Differences Between Modules

The IPS module for the ASA 5510 and higher supports higher performance requirements, while the IPS module for the ASA 5505 is designed for a small office installation. The following features are supported for the ASA 5510 and higher, and not for the ASA 5505:

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

Licensing Requirements for the IPS Module

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

The IPS application on the 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 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. For a complete list of supported ASA software, models, and modules, see *Cisco ASA 5500 Series Hardware and Software Compatibility*:

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

- 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 IPS Module

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

- IPS Module Task Overview, page 59-5
- Configuring the Security Policy on the IPS Module, page 59-5
- Assigning Virtual Sensors to a Security Context (ASA 5510 and Higher), page 59-6
- Diverting Traffic to the IPS Module, page 59-8

IPS Module Task Overview

Configuring the IPS module 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 IPS module, perform the following steps:

Step 1 On the IPS module, configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. (ASA 5510 and higher) Configure the inspection and protection policy for each virtual sensor if you want to run the IPS module in multiple sensor mode. See the "Configuring the Security Policy on the IPS Module" section on page 59-5.

Step 2 (ASA 5510 and higher) 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 59-6.

Step 3 On the ASA, identify traffic to divert to the IPS module. See the "Diverting Traffic to the IPS Module" section on page 59-8.

Configuring the Security Policy on the IPS Module

This section describes how to access the IPS application in the IPS module.

Note You can alternatively use ASDM to configure the IPS module. See the ASDM documentation for more information.

See also the "Configuring the SSC Management Interface" section on page 58-4 to configure the SSC management interface for ASDM access and other uses.

Detailed Steps

Step 1 Session from the ASA to the IPS module. See the "Sessioning to the Module" section on page 58-6

Step 2 To run the setup utility for initial configuration of the IPS module, enter the following command:

```
sensor# setup
```

You are prompted for basic settings.

Step 3 Configure the IPS security policy.

(ASA 5510 and higher) 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 ASA does not specify a virtual sensor name in its configuration, the default sensor is used.

Because the IPS software that runs on the IPS module 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

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

```
sensor# exit
```

If you sessioned to the 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 59-6.

For the ASA in single context mode, see the "Diverting Traffic to the IPS Module" section on page 59-8.

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 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 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 a Security Context" section on page 5-16.

Detailed Steps

	Command	Purpose

Step 1	**context** *name*
	
	Example:
	`hostname(config)# context admin`
	`hostname(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:** `hostname(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 IPS module. To view the sensors that are configured on the 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 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 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 on the IPS module.
Step 3	**changeto context** *context_name* **Example:** `hostname# changeto context customer1`	Changes to the context so you can configure the IPS security policy as described in "Diverting Traffic to the IPS Module" section on page 59-8.

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 IPS module is used.

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

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

hostname(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 IPS Module" section on page 59-8.

Diverting Traffic to the IPS Module

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

Prerequisites

In multiple context mode, perform these steps in each context execution space.

Detailed Steps

	Command	Purpose
Step 1	**class-map** *name* **Example:** `hostname(config)# class-map ips_class`	Creates a class map to identify the traffic for which you want to send to the IPS module. If you want to send multiple traffic classes to the IPS module, you can create multiple class maps for use in the security policy.
Step 2	**match** *parameter* **Example:** `hostname(config-cmap)# match access-list ips_traffic`	Specifies the traffic in the class map. See the "Identifying Traffic (Layer 3/4 Class Map)" section on page 9-13 for more information.

	Command	Purpose
Step 3	**policy-map** *name* **Example:** `hostname(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:** `hostname(config-pmap)# class ips_class`	Identifies the class map you created in Step 1.
Step 5	**ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}] **Example:** `hostname(config-pmap-c)# ips promiscuous fail-close`	Specifies that the traffic should be sent to the IPS module. The **inline** and **promiscuous** keywords control the operating mode of the IPS module. See the "Operating Modes" section on page 59-2 for more details. The **fail-close** keyword sets the adaptive security appliance to block all traffic if the IPS module is unavailable. The **fail-open** keyword sets the adaptive security appliance to allow all traffic through, uninspected, if the 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 ... 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 59-6). 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 IPS module. If you enter a name that does not yet exist on the IPS module, you get an error, and the command is rejected.
Step 6	(Optional) **class** *name2* **Example:** `hostname(config-pmap)# class ips_class2`	If you created multiple class maps for IPS traffic, you can specify another class for the policy. See the "Information About Layer 3/4 Policy Maps" section on page 9-5 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:** hostname(config-pmap-c)# ips promiscuous fail-close	Specifies that the second class of traffic should be sent to the IPS module.
Step 8	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **Example:** hostname(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.

Monitoring the IPS Module

See the "Monitoring SSMs and SSCs" section on page 58-9.

Configuration Examples for the IPS Module

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

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(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 IPS module in inline mode, and allows all traffic through if the IPS module fails for any reason. For the my-ips-class traffic, sensor1 is used; for the my-ips-class2 traffic, sensor2 is used.

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
hostname(config)# class-map my-ips-class2
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface outside
```

Feature History for the IPS Module

Table 59-1 lists the release history for this feature.

Table 59-1 Feature History for the IPS Module

Feature Name	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 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 IPS SSP-10, -20, -40, and -60 for the ASA 5585-X	8.2(4.4)	We introduced support for the IPS SSP-10, -20, -40, and -60 for the ASA 5585-X. You can only install the IPS SSP with a matching-level SSP; for example, SSP-10 and IPS SSP-10.