



Configuring the AIP SSM

The optional AIP SSM runs advanced IPS software that provides further security inspection either in inline mode or promiscuous mode. The adaptive security appliance diverts packets to the AIP SSM just before the packet exits the egress interface (or before VPN encryption occurs, if configured) and after other firewall policies are applied. For example, packets that are blocked by an access list are not forwarded to the AIP SSM.

If you purchased an AIP SSM, use the procedures in this chapter to:

- Configure the adaptive security appliance to identify traffic to be diverted to the AIP SSM
- Session in to the AIP SSM and run setup



Note

The AIP SSM is supported in ASA software versions 7.01 and later.

This chapter includes the following sections:

- [AIP SSM Configuration, page 9-1](#)
- [What to Do Next, page 9-7](#)

AIP SSM Configuration

This procedure describes the configuration steps you must take to configure the adaptive security appliance for AIP SSM.

This section includes the following topics:

- [Overview of Configuration Process, page 9-2](#)
- [Configuring the ASA 5500 to Divert Traffic to the AIP SSM, page 9-2](#)
- [Sessioning to the AIP SSM and Running Setup, page 9-5](#)

Overview of Configuration Process

Configuring the AIP SSM is a three-part process that involves configuration of the adaptive security appliance first, then configuration of the AIP SSM, and then the configuration of the IPS software:

1. On the ASA 5500 series adaptive security appliance, identify traffic to divert to the AIP SSM (as described in the [“Configuring the ASA 5500 to Divert Traffic to the AIP SSM”](#) section on page 9-2).
2. 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.
3. Configure the IPS software that runs on the AIP SSM. Information about the IPS software is beyond the scope of this document. Detailed information about IPS software configuration is available in the following separate documentation that came with your IPS product:
 - [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface](#)
 - [Cisco Intrusion Prevention System Command Reference](#)

Configuring the ASA 5500 to Divert Traffic to the AIP SSM

You use MPF (Modular Policy Framework) commands to configure the adaptive security appliance to divert traffic to the AIP SSM. This procedure provides sufficient information to configure a simple set of policies in an AIP SSM deployment. If you want to create a more complex set of policies, read the Modular Policy Framework chapter in *Cisco Security Appliance Command Line Configuration Guide* which introduces Modular Policy Framework concepts and common commands.

To identify traffic to divert from the adaptive security appliance to the AIP SSM, perform the following steps:

- Step 1** Create an access list that matches all traffic:

```
hostname(config)# access-list acl-name permit ip any any
```

- Step 2** Create a class map to identify the traffic that should be diverted to the AIP SSM. Use the **class-map** command to do so, as follows:

```
hostname(config)# class-map class_map_name  
hostname(config-cmap)#
```

where *class_map_name* is the name of the traffic class. When you enter the **class-map** command, the CLI enters class map configuration mode.

- Step 3** With the access list you created in [Step 1](#), use a **match access-list** command to identify the traffic to be scanned:

```
hostname(config-cmap)# match access-list acl-name
```

- Step 4** Create a policy map or modify an existing policy map that you want to use to send traffic to the AIP SSM. To do so, use the **policy-map** command, as follows:

```
hostname(config-cmap)# policy-map policy_map_name  
hostname(config-pmap)#
```

where *policy_map_name* is the name of the policy map. The CLI enters the policy map configuration mode and the prompt changes accordingly.

- Step 5** Specify the class map, created in [Step 2](#), that identifies the traffic to be scanned. Use the **class** command to do so, as follows:

```
hostname(config-pmap)# class class_map_name  
hostname(config-pmap-c)#
```

where *class_map_name* is the name of the class map you created in [Step 2](#). The CLI enters the policy map class configuration mode and the prompt changes accordingly.

- Step 6** Assign the traffic identified by the class map as traffic to be sent to the AIP SSM. Use the **ips** command to do so, as follows:

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |  
fail-open}
```

The **inline** and **promiscuous** keywords control the operating mode of the AIP SSM. The **fail-close** and **fail-open** keywords control how the adaptive security appliance treats traffic when the AIP SSM is unavailable. For more information about the operating modes and failure behavior, see the “AIP SSM Configuration” section on page 9-1.

- Step 7** Use the **service-policy** command to apply the policy map globally or to a specific interface, as follows:

```
hostname(config-pmap-c)# service-policy policy_map_name [global |
interface interface_ID]
hostname(config)#
```

where *policy_map_name* is the policy map you configured in Step 4. If you want to apply the policy map to traffic on all the interfaces, use the **global** keyword. If you want to apply the policy map to traffic on a specific interface, use the **interface** *interface_ID* option, where *interface_ID* is the name assigned to the interface with the **nameif** command.

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.

The adaptive security appliance begins diverting traffic to the AIP SSM as specified.

The following example diverts all IP traffic to the AIP SSM in promiscuous mode, and blocks all IP traffic should the AIP SSM card fail 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
```

Sessioning to the AIP SSM and Running Setup

After you have completed configuration of the ASA 5500 series adaptive security appliance to divert traffic to the AIP SSM, session to the AIP SSM and run the setup utility for initial configuration.

**Note**

You can either session to the SSM from the adaptive security appliance (by using the **session 1** command) or you can connect directly to the SSM using SSH or Telnet on its management interface. Alternatively, you can use ASDM.

To session to the AIP SSM from the adaptive adaptive security appliance, perform the following steps:

- Step 1** Enter the **session 1** command to session from the ASA 5500 series adaptive security appliance to the AIP SSM:

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

- Step 2** Enter the username and password. The default username and password are both **cisco**:



Note The first time you log in to the AIP SSM you are prompted to change the default password. Passwords must be at least eight characters long and *not* a dictionary word.

```
login: cisco
Password:
Last login: Fri Sep  2 06:21:20 from xxx.xxx.xxx.xxx
***NOTICE***
This product contains cryptographic features and is subject to United
States
and local country laws governing import, export, transfer and use.
Delivery
of Cisco cryptographic products does not imply third-party authority
to import,
export, distribute or use encryption. Importers, exporters,
distributors and
users are responsible for compliance with U.S. and local country laws.
By using
```

this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

LICENSE NOTICE

There is no license key installed on the system.

Please go to <http://www.cisco.com/go/license>

to obtain a new license or install a license.

AIP SSM#



Note

If you see the license notice above (which displays only is some versions of software), you can ignore the message until you need to upgrade the signature files on the AIP SSM. The AIP SSM continues to operate at the current signature level until a valid license key is installed. You can install the license key at a later time. The license key does not affect the current functionality of the AIP SSM.

Step 3

Enter the **setup** command to run the setup utility for initial configuration of the AIP SSM:

AIP SSM# **setup**

What to Do Next

You are now ready to configure the adaptive security appliance for intrusion prevention. Use the following documents to continue configuring the adaptive security appliance for your implementation.

To Do This ...	See ...
Configure the IPS sensor	<i>Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface</i> <i>Cisco Intrusion Prevention System Command Reference</i>
Optimize performance by creating more efficient service policies	“Managing AIP SSM and CSC SSM” in <i>Cisco Security Appliance Command Line Configuration Guide</i>

After you have configured the IPS sensory and AIP SSM software, you may want to consider performing some of the following additional steps:

To Do This ...	See ...
Refine configuration and configure optional and advanced features	<i>Cisco Security Appliance Command Line Configuration Guide</i>
Learn about daily operations	<i>Cisco Security Appliance Command Reference</i> <i>Cisco Security Appliance Logging Configuration and System Log Messages</i>
Review hardware maintenance and troubleshooting information	<i>Cisco ASA 5500 Series Hardware Installation Guide</i>

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This ...	See ...
Configure protection of a DMZ web server	Chapter 6, “Scenario: DMZ Configuration”
Configure a remote-access VPN	Chapter 7, “Scenario: Remote-Access VPN Configuration”
Configure a site-to-site VPN	Chapter 8, “Scenario: Site-to-Site VPN Configuration”