



CHAPTER 14

Configuring AIP-SSM

This chapter contains procedures that are specific to configuring AIP-SSM. It contains the following sections:

- [Configuration Sequence, page 14-1](#)
- [Verifying AIP-SSM Initialization, page 14-2](#)
- [Sending Traffic to AIP-SSM, page 14-2](#)
- [Reloading, Shutting Down, Resetting, and Recovering AIP-SSM, page 14-5](#)

Configuration Sequence

Perform the following tasks to configure AIP-SSM:

1. Log in to AIP-SSM.
For the procedure, see [Logging In to AIP-SSM, page 2-7](#).
2. Initialize AIP-SSM.
Run the **setup** command to initialize AIP-SSM.
For the procedure, see [Initializing the Sensor, page 3-2](#).
3. Verify the AIP-SSM initialization.
For the procedure, see [Verifying AIP-SSM Initialization, page 14-2](#).
4. Configure ASA to send IPS traffic to AIP-SSM.
For the procedure, see [Sending Traffic to AIP-SSM, page 14-2](#).
5. Perform other initial tasks, such as adding users, trusted hosts, and so forth.
For the procedures, see [Chapter 4, “Initial Configuration Tasks.”](#)
6. Configure intrusion prevention.
For the procedures, see [Chapter 6, “Configuring Event Action Rules,”](#) [Chapter 7, “Defining Signatures,”](#) and [Chapter 10, “Configuring Blocking.”](#)
7. Perform miscellaneous tasks to keep your AIP-SSM running smoothly.
For the procedures, see [Chapter 13, “Administrative Tasks for the Sensor.”](#)

8. Upgrade the IPS software with new signature updates and service packs.
For more information, see [Obtaining Cisco IPS Software, page 18-1](#).
9. Reimage AIP-SSM when needed.
For the procedure, see [Installing the AIP-SSM System Image, page 17-37](#).

Verifying AIP-SSM Initialization

You can use the **show module slot details** command to verify that you have initialized AIP-SSM and to verify that you have the correct software version.

To verify initialization, follow these steps:

Step 1 Log in to ASA.

Step 2 Obtain the details about AIP-SSM:

```
hostname# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:                AIP-SSM-20
Hardware version:     0.2
Serial Number:        P2B000005D0
Firmware version:     1.0(10)0
Software version:     5.0(0.27)S129.0
Status:               Up
Mgmt IP addr:         10.89.149.219
Mgmt web ports:       881
Mgmt TLS enabled:     false
hostname#
```

Step 3 Confirm the information. If you need to change anything, for the tasks you need to perform to update AIP-SSM settings, see [Configuration Sequence, page 14-1](#).

Sending Traffic to AIP-SSM

This section describes how to configure AIP-SSM to receive IPS traffic from ASA (inline or promiscuous mode), and contains the following sections:

- [Overview, page 14-2](#)
- [Configuring ASA to Send IPS Traffic to AIP-SSM, page 14-3](#)

Overview

ASA diverts packets to 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 AIP-SSM.

You can configure AIP-SSM to inspect traffic in inline or promiscuous mode and in fail-open or fail-over mode.

On ASA, to identify traffic to be diverted to and inspected by AIP-SSM:

1. Use the **class-map** command to define the IPS traffic class.
2. Use the **policy-map** command to create an IPS policy map by associating the traffic class with one or more actions.
3. Use the **service-policy** command to create an IPS security policy by associating the policy map with one or more interfaces.

You can use the ASA CLI or ASDM to configure IPS traffic inspection.

Configuring ASA to Send IPS Traffic to AIP-SSM



Note

For more information on these commands, refer to Chapter 18, “Using Modular Policy Framework,” in *Cisco Security Appliance Command Line Configuration Guide*.

The following options apply:

- **access-list** *word*—Configures an access control element; *word* is the access list identifier (up to 241 characters).
- **class-map** *class_map_name*—Defines the IPS traffic class.
- **match**—Identifies the traffic included in the traffic class.

A traffic class map contains a **match** command. When a packet is matched against a class map, the match result is either a match or a no match.

- **access-list**—Matches an access list.
- **any**—Matches any packet.
- **policy-map** *policy_map_name*—Creates an IPS policy map by associating the traffic class with one or more actions.
- **ips [inline | promiscuous] [fail-close | fail-open]**—Assigns traffic to AIP-SSM:
 - **inline**—Places AIP-SSM directly in the traffic flow.
No traffic can continue through ASA without first passing through, and being inspected by, AIP-SSM. This mode is the most secure because every packet is analyzed before being permitted through. Also, AIP-SSM can implement a blocking policy on a packet-by-packet basis. This mode, however, can affect throughput.
 - **promiscuous**—Sends a duplicate stream of traffic to AIP-SSM.
This mode is less secure, but has little impact on traffic throughput. Unlike inline mode, AIP-SSM can only block traffic by instructing ASA to block the traffic or by resetting a connection on ASA. Moreover, while AIP-SSM is analyzing the traffic, a small amount of traffic might pass through ASA before AIP-SSM can block it.
 - **fail-close**—Sets ASA to block all traffic if AIP-SSM is unavailable.
 - **fail-open**—Sets ASA to permit all traffic through, uninspected, if AIP-SSM is unavailable.
- **service-policy** *service_policy_name* [**global** | **interface** *interface_name*]—Creates an IPS security policy by associating the policy map with one or more interfaces.
 - **global**—Applies the policy map to all interfaces.

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.

- **interface**—Applies the policy to one interface.

To send traffic from ASA to AIP-SSM for the IPS to inspect, follow these steps:

-
- Step 1** Log in to ASA.
- Step 2** Enter configuration mode:
asa# **configure terminal**
- Step 3** Create an IPS access list:
asa(config)# **access-list IPS permit ip any any**
- Step 4** Define the IPS traffic class:
asa(config)# **class-map class_map_name**
asa(config-cmap)# **match [access-list | any]**
- Step 5** Define the IPS policy map:
asa(config-cmap)# **policy-map policy_map_name**
- Step 6** Identify the class map from Step 4 to which you want to assign an action:
asa(config-pmap)# **class class_map_name**
- Step 7** Assign traffic to AIP-SSM:
asa(config-pmap-c)# **ips [inline | promiscuous] [fail-close | fail-open]**
- Step 8** Define the IPS service policy:
asa(config-pmap-c)# **service-policy policymap_name [global | interface interface_name]**
- Step 9** Verify the settings:
asa(config-pmap-c)# **show running-config**
!
class-map my_ips_class
class-map my-ips-class
 match access-list IPS
class-map all_traffic
 match access-list all_traffic
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map my-ids-policy
 class my-ips-class
 ips promiscuous fail-close
 !
service-policy my-ids-policy global
- Step 10** Exit and save the configuration:
asa(config-pmap-c)# **exit**
asa(config-pmap)# **exit**
asa(config)# **exit**
asa#

The following example diverts all IP traffic to AIP-SSM in promiscuous mode, and blocks all IP traffic should AIP-SSM fail for any reason:

```
asa(config)# access-list IPS permit ip any any
asa(config)# class-map my-ips-class
asa(config-cmap)# match access-list IPS
asa(config-cmap)# policy-map my-ids-policy
asa(config-pmap)# class my-ips-class
asa(config-pmap-c)# ips promiscuous fail-close
asa(config-pmap-c)# service-policy my-ids-policy global
```

Reloading, Shutting Down, Resetting, and Recovering AIP-SSM

Use the following commands to reload, shut down, reset, and recover AIP-SSM directly from ASA:



Note

You can enter the **hw-module** commands from privileged EXEC mode or from global configuration mode. You can enter the commands in single routed mode and single transparent mode. For adaptive security devices operating in multi-mode (routed or transparent multi-mode) you can only execute the **hw-module** commands from the system context (not from administrator or user contexts).

- **hw-module module 1 reload**

This command reloads the software on AIP-SSM without doing a hardware reset. It is effective only when AIP-SSM is in the Up state.

- **hw-module module 1 shutdown**

This command shuts down the software on AIP-SSM. It is effective only when AIP-SSM is in Up state.

- **hw-module module 1 reset**

This command performs a hardware reset of AIP-SSM. It is applicable when the card is in the Up/Down/Unresponsive/Recover states.

- **hw-module module 1 recover [boot | stop | configure]**

The **recover** command displays a set of interactive options for setting or changing the recovery parameters. You can change the parameter or keep the existing setting by pressing **Enter**.

For the procedure for recovering AIP-SSM, see [Installing the AIP-SSM System Image, page 17-37](#).

- **hw-module module 1 recover boot**

This command initiates recovery of AIP-SSM. It is applicable only when AIP-SSM is in the Up state.

- **hw-module module 1 recover stop**

This command stops recovery of AIP-SSM. It is applicable only when AIP-SSM is in the Recover state.



Caution

If AIP-SSM recovery needs to be stopped, you must issue the **hw-module module 1 recover stop** command within 30 to 45 seconds after starting AIP-SSM recovery. Waiting any longer can lead to unexpected consequences, for example, AIP-SSM may come up in the Unresponsive state.

- hw-module module 1 recover configure

Use this command to configure parameters for module recovery. The essential parameters are the IP address and recovery image TFTP URL location.

Example:

```
asa# hw-module module 1 recover configure
Image URL [tftp://1.1.1.1/IPS-SSM-K9-sys-1.1-a-5.0-0.15-S91-0.15.img]:
Port IP Address [1.1.1.23]:
VLAN ID [0]:
Gateway IP Address [0.0.0.0]:1.1.1.2
hostname#

asa# show module 1 recover
Module 1 recover parameters...
Boot Recovery Image: No
Image URL:          tftp://1.1.1.1/IPS-SSM-K9-sys-1.1-a-5.0-0.15-S91-0.15.img
Port IP Address:    1.1.1.23
Gateway IP Address: 1.1.1.2
VLAN ID:            0
```