Configuring the ASA 5500 AIP SSM

This chapter contains procedures that are specific to configuring the ASA 5500 AIP SSM. It contains the following sections:

ASA 5500 AIP SSM Notes and Caveats

The following notes and caveats apply to configuring the ASA 5500 AIP SSM:

- All IPS platforms allow ten concurrent CLI sessions.
- Cisco Adaptive Security Appliance Software 7.2.3 or later supports virtualization.
- The **allocate-ips** command does not apply to single mode. In this mode, the adaptive security appliance accepts any virtual sensor named in a **policy-map** command.
- Anomaly detection is disabled by default in IPS 7.1(2)E4 and later. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.
- You cannot allocate the same virtual sensor twice in a context.
- You can only configure one default virtual sensor per context. You must turn off the default flag of an existing default virtual sensor before you can designate another virtual sensor as the default.

- IPS appliances reset both the attacker and victim when the Reset TCP Connection is selected and they reset the victim when Deny Connection Inline is selected. For the ASA IPS modules, TCP resets are sent by the ASA. The ASA resets the server, which in some cases is the attacker and in others the victim. The ASA does not always reset the client. The TCP RST packet, which is automatically generated with a reset action, should be sent to both the target and the attacker. However, when the ASA IPS modules are in inline mode, and when signature 6251/0 is triggered, the RST packet generated by Reset TCP Connection is sent to the attacker only.

TCP Reset Differences Between IPS Appliances and ASA IPS Modules

The IPS appliance sends TCP reset packets to both the attacker and victim when reset-tcp-connection is selected. The IPS appliance sends a TCP reset packet only to the victim under the following circumstances:

- When a deny-packet-inline or deny-connection-inline is selected
- When TCP-based signatures and reset-tcp-connection have NOT been selected

In the case of the ASA 5500 AIP SSM, the TCP reset request is sent to the ASA, and then the ASA sends the TCP reset packets. The ASA sends TCP reset packets to both the attacker and victim when the reset-tcp-connection is selected. When deny-packet-inline or deny-connection-inline is selected, the ASA sends the TCP reset packet to either the attacker or victim depending on the configuration of the signature. Signatures configured to swap the attacker and victim when reporting the alert can cause the ASA to send the TCP reset packet to the attacker.

Reloading IPS Messages

The following messages generated during some IPS signature and global correlation updates for IPS 7.1 and later on the ASA 5500 AIP SSM can cause confusion since the IPS is not reloading:

```
ASA5585-SSP-IPS20 Module in slot 1, application up "IPS", version "7.1(1)E4" Normal
Operation
ASA5585-SSP-IPS20 Module in slot 1, application reloading "IPS", version "7.1(1)E4" Config
Change
```

These messages are generated during some, but not all, of the global correlation updates that are attempted every five minutes. This is expected behavior. There is a global correlation check every five minutes, but there may not be an update available, thus the message appears every hour or so. When a global correlation update actually takes place, a message is sent from the IPS to the ASA indicating that a configuration change is taking place.

ASA 5500 AIP SSM Configuration Sequence

Perform the following tasks to configure the ASA 5500 AIP SSM:

1. Obtain and install the current IPS software if your software is not up to date.
2. Obtain and install the license key.
3. Log (session) in to the ASA 5500 AIP SSM.
4. Run the **setup** command to initialize the ASA 5500 AIP SSM.
5. Verify initialization for the ASA 5500 AIP SSM.
6. (Optional) If you have Cisco Adaptive Security Appliance Software 7.2.3 or later, configure multiple virtual sensors.
7. Configure the adaptive security appliance to send IPS traffic to the ASA 5500 AIP SSM.
8. Perform other initial tasks, such as adding users, trusted hosts, and so forth.

9. Configure intrusion prevention.
10. Configure global correlation.
11. Configure global correlation.
12. Perform miscellaneous tasks to keep your ASA 5500 AIP SSM running smoothly.
13. Upgrade the IPS software with new signature updates and service packs as they become available.
14. Reimage the ASA 5500 AIP SSM when needed.

For More Information

- For the procedure for logging in to the ASA 5500 AIP SSM, see Chapter 2, "Logging In to the Sensor."
- For the procedure for running the **setup** command, see Advanced Setup for the ASA 5500 AIP SSM, page 3-14.
- For the procedure for verifying ASA 5500 AIP SSM initialization, see Verifying ASA 5500 AIP SSM Initialization, page 18-3.
- For the procedure for creating virtual sensors, see Creating Virtual Sensors for the ASA 5500 AIP SSM, page 18-4.
- For the procedure for configuring ASA to send traffic to the ASA 5500 AIP SSM, see Sending Traffic to the ASA 5500 AIP SSM, page 18-10.
- For the procedures for setting up the sensor, see Chapter 4, "Setting Up the Sensor."
- For the procedures for configuring intrusion prevention, see Chapter 7, "Configuring Event Action Rules," Chapter 8, "Defining Signatures," Chapter 9, "Configuring Anomaly Detection,"and Chapter 14, "Configuring Attack Response Controller for Blocking and Rate Limiting."
- For the procedures for configuring global correlation, see Chapter 10, "Configuring Global Correlation."
- For the procedures for keeping your ASA 5500 AIP SSM running smoothly, see Chapter 17, "Administrative Tasks for the Sensor."
- For more information on how to obtain Cisco IPS software, see Chapter 21, "Obtaining Software."
- For the procedure for reimaging the ASA 5500 AIP SSM, see Installing the System Image for the ASA 5500 AIP SSM, page 22-28.

Verifying ASA 5500 AIP SSM Initialization

You can use the **show module** *slot* **details** command to verify that you have initialized the ASA 5500 AIP SSM and to verify that you have the correct software version.

To verify initialization, follow these steps:

Step 1 Log in to the adaptive security appliance.

Step 2 Obtain the details about the ASA 5500 AIP SSM.

```
asa# show module 1 details
ASA 5500 Series Security Services Module-10
Model:              ASA-SSM-10
Hardware version:   1.0
Serial Number:      JAB09370212
Firmware version:   1.0(10)0
```

```
Software version:   7.0(1)E3
MAC Address Range:  0012.d948.fe73 to 0012.d948.fe73
App. name:          IPS
App. Status:        Up
App. Status Desc:
App. version:       6.2(1)E3
Data plane Status:  Up
Status:             Up
Mgmt IP addr: 171.69.36.171
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

Step 3 Confirm the information.

Creating Virtual Sensors for the ASA 5500 AIP SSM

Note Cisco Adaptive Security Appliance Software 7.2.3 or later supports virtualization.

This section describes how to create virtual sensors on the ASA 5500 AIP SSM, and contains the following topics:

ASA 5500 AIP SSM and Virtualization

The ASA 5500 AIP SSM has one sensing interface, GigabitEthernet 0/1. When you create multiple virtual sensors, you must assign this interface to only one virtual sensor. For the other virtual sensors you do not need to designate an interface.

After you create virtual sensors, you must map them to a security context on the adaptive security appliance using the **allocate-ips** command. You can map many security contexts to many virtual sensors.

Note The **allocate-ips** command does not apply to single mode. In this mode, the adaptive security appliance accepts any virtual sensor named in a **policy-map** command.

The **allocate-ips** command adds a new entry to the security context database. A warning is issued if the specified virtual sensor does not exist; however, the configuration is allowed. The configuration is checked again when the **service-policy** command is processed. If the virtual sensor is not valid, the **fail-open** policy is enforced.

ASA 5500 AIP SSM Virtual Sensor Configuration Sequence

Follow this sequence to create virtual sensors on the ASA 5500 AIP SSM, and to assign them to adaptive security appliance contexts:

1. Configure up to four virtual sensors.
2. Assign the ASA 5500 AIP SSM sensing interface (GigabitEthernet 0/1) to one of the virtual sensors.
3. (Optional) Assign virtual sensors to different contexts on the adaptive security appliance.
4. Use MPF to direct traffic to the targeted virtual sensor.

Creating Virtual Sensors

Note You can create four virtual sensors.

Use the **virtual-sensor** *name* command in service analysis engine submode to create virtual sensors on the ASA 5500 AIP SSM. You assign policies (anomaly detection, event action rules, and signature definition) to the virtual sensor. You can use the default policies, ad0, rules0, or sig0, or you can create new policies.Then you assign the sensing interface, GigabitEthernet 0/1 for the ASA 5500 AIP SSM to one virtual sensor.

The following options apply:

- **anomaly-detection**—Specifies the anomaly detection parameters:
  - **anomaly-detection-name** *name*—Specifies the name of the anomaly detection policy.
  - **operational-mode**—Specifies the anomaly detection mode (**inactive**, **learn**, **detect**).

    Note Anomaly detection is disabled by default in IPS 7.1(2)E4 and later. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

- **description**—Provides a description of the virtual sensor.
- **event-action-rules**—Specifies the name of the event action rules policy.
- **signature-definition**—Specifies the name of the signature definition policy.
- **physical-interfaces**—Specifies the name of the physical interface.
- **no**—Removes an entry or selection.

Creating Virtual Sensors

To create a virtual sensor on the ASA 5500 AIP SSM, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter service analysis mode.

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

Step 3 Add a virtual sensor.

```
sensor(config-ana)# virtual-sensor vs1
sensor(config-ana-vir)#
```

Step 4 Add a description for this virtual sensor.

```
sensor(config-ana-vir)# description virtual sensor 1
```

Step 5 Assign an anomaly detection policy and operational mode to this virtual sensor if you have enabled anomaly detection. If you do not want to use the default anomaly detection policy, ad0, you must create a new one using the **service anomaly-detection** *name* command, for example, ad1.

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# anomaly-detection-name ad0
sensor(config-ana-vir-ano)# operational-mode learn
```

Step 6 Assign an event action rules policy to this virtual sensor. If you do not want to use the default event action rules policy, rules0, you must create a new one using the **service event-action-rules** *name* command, for example, rules1

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# event-action-rules rules0
```

Step 7 Assign a signature definition policy to this virtual sensor. If you do not want to use the default signature definition policy, sig0, you must create a new one using the **service signature-definition** *name* command, for example sig1.

```
sensor(config-ana-vir)# signature-definition sig0
```

Step 8 Assign the interface to one virtual sensor. By default the sensing interface is already assigned to the default virtual sensor, vs0. You must remove it from the default virtual sensor to assign it to another virtual sensor that you create.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/1
```

Step 9 Verify the virtual sensor settings.

```
sensor(config-ana-vir)# show settings
   name: vs1
   -----------------------------------------------
      description: virtual sensor 1 default:
      signature-definition: sig1 default: sig0
      event-action-rules: rules1 default: rules0
      anomaly-detection
      -----------------------------------------------
         anomaly-detection-name: ad1 default: ad0
         operational-mode: learn default: detect
      -----------------------------------------------
      physical-interface (min: 0, max: 999999999, current: 2)
      -----------------------------------------------
         name: GigabitEthernet0/1
         subinterface-number: 0 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      logical-interface (min: 0, max: 999999999, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
sensor(config-ana-vir)#
```

Step 10 Exit analysis engine mode.

```
sensor(config-ana-vir)# exit
```

```
sensor(config-ana)# exit
Apply Changes:?[yes]:
sensor(config)#
```

Step 11 Press **Enter** to apply the changes or enter **no** to discard them.

For More Information

- For the procedures for creating and configuring anomaly detection policies, see Working With Anomaly Detection Policies, page 9-9.
- For the procedure for creating and configuring event action rules policies, see Working With Event Action Rules Policies, page 7-8.
- For the procedure for creating and configuring signature definitions, Working With Signature Definition Policies, page 8-2.

Assigning Virtual Sensors to Adaptive Security Appliance Contexts

After you create virtual sensors on the ASA 5500 AIP SSM, you must assign the virtual sensors to a security context on the adaptive security appliance.

The following options apply:

- **[no] allocate-ips** *sensor_name* [*mapped_name*] [**default**]—Allocates a virtual sensor to a security context. Supported modes are multiple mode, system context, and context submode.

  Note You cannot allocate the same virtual sensor twice in a context.

  - *sensor_name*—Specifies the name of the virtual sensor configured on the ASA 5500 AIP SSM. You receive a warning message if the name is not valid.
  - *mapped_name*—Specifies the name by which the security context knows the virtual sensor.

    Note The mapped name is used to hide the real name of the virtual sensor from the context, usually done for reasons of security or convenience to make the context configuration more generic. If no mapped name is used, the real virtual sensor name is used. You cannot reuse a mapped name for two different virtual sensors in a context.

  - **no**—De-allocates the sensor, looks through the policy map configurations, and deletes any IPS subcommand that refers to it.
  - **default**—Specifies this virtual sensor as the default. All legacy IPS configurations that do not specify a virtual sensor are mapped to this virtual sensor.

Caution You can only configure one default virtual sensor per context. You must turn off the default flag of an existing default virtual sensor before you can designate another virtual sensor as the default.

  - **clear configure allocate-ips**—Removes the configuration.
  - **allocate-ips?**—Displays the list of configured virtual sensors.

- **show context** [**detail**]—Updated to display information about virtual sensors. In user context mode, a new line is added to show the mapped names of all virtual sensors that have been allocated to this context. In system mode, two new lines are added to show the real and mapped names of virtual sensors allocated to this context.

You can assign multiple virtual sensors to a context. Multiple contexts can share one virtual sensor, and when sharing, the contexts can have different mapped names (aliases) for the same virtual sensor. The following procedure demonstrates how to add three security contexts in multiple mode and how to assign virtual sensors to these security contexts.

Assigning Virtual Sensors to Contexts

To assign virtual sensors to adaptive security appliance contexts in multiple mode for the ASA 5500 AIP SSM, follow these steps:

Step 1 Log in to the adaptive security appliance.

Step 2 Display the list of available virtual sensors.

```
asa# show ips
Sensor Name      Sensor ID
-----------      ---------
vs0              1
vs1              2
asa#
```

Step 3 Enter configuration mode.

```
asa# configure terminal
asa(config)#
```

Step 4 Enter multiple mode.

```
asa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] yes
asa(config)#
```

Step 5 Add three context modes to multiple mode.

```
asa(config)# admin-context admin
Creating context 'admin'... Done. (13)
asa(config)# context admin
asa(config-ctx)#   allocate-interface GigabitEthernet0/0.101
asa(config-ctx)#   allocate-interface GigabitEthernet0/1.102
asa(config-ctx)#   allocate-interface Management0/0
asa(config-ctx)#   config-url disk0:/admin.cfg
Cryptochecksum (changed): 0c34dc67 f413ad74 e297464a db211681
INFO: Context admin was created with URL disk0:/admin.cfg
INFO: Admin context will take some time to come up .... please wait.
asa(config-ctx)#
asa(config-ctx)# context c2
Creating context 'c2'... Done. (14)
asa(config-ctx)#   allocate-interface GigabitEthernet0/0.103
asa(config-ctx)#   allocate-interface GigabitEthernet0/1.104
asa(config-ctx)#   config-url disk0:/c2.cfg

WARNING: Could not fetch the URL disk0:/c2.cfg
INFO: Creating context with default config
asa(config-ctx)#
asa(config-ctx)# context c3
Creating context 'c3'... Done. (15)
```

```
asa(config-ctx)# all
asa(config-ctx)# allocate-in
asa(config-ctx)# allocate-interface g0/2
asa(config-ctx)# allocate-interface g0/3
asa(config-ctx)#   config-url disk0:/c3.cfg

WARNING: Could not fetch the URL disk0:/c3.cfg
INFO: Creating context with default config
asa(config-ctx)#
```

Step 6 Assign virtual sensors to the security contexts.

```
asa(config)# context admin
asa(config-ctx)#   allocate-ips vs0 adminvs0
asa(config-ctx)# exit
asa(config)# context c2
asa(config-ctx)#   allocate-ips vs1 c2vs1
asa(config)# context c3
asa(config-ctx)# allocate-ips vs0 c3vs0
asa(config-ctx)# allocate-ips vs1 c3vs1
asa(config-ctx)#
```

Step 7 Configure MPF for each context.

Note The following example shows context 3 (c3).

```
asa(config)# context c3
asa/c3(config)# class-map any
asa/c3(config-cmap)# match access-list any
asa/c3(config-cmap)# exit
asa/c3(config)# policy-map ips_out
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips promiscuous fail-close sensor c3vs1
asa/c3(config-pmap-c)# policy-map ips_in
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips inline fail-open sensor c3vs0
asa/c3(config-pmap-c)# service-policy ips_out interface outside
asa/c3(config)# service-policy ips_in interface inside
asa/c3(config)#
```

Step 8 Confirm the configuration.

```
asa/c3(config)# exit
asa(config)# show ips detail
Sensor Name      Sensor ID        Allocated To     Mapped Name
-----------      ---------        ------------     -----------
vs0              1                admin            adminvs0
                                  c3               c3vs0
vs1              2                c2               c2vs1
                                  c3               c3vs1
asa(config)#
```

Sending Traffic to the ASA 5500 AIP SSM

Note This section applies to Cisco Adaptive Security Appliance Software 7.2 or earlier for ASA 5500 AIP SSM.

This section describes how to configure ASA 5500 AIP SSM to receive IPS traffic from the adaptive security appliance (inline or promiscuous mode) if it is running Cisco Adaptive Security Appliance Software 7.2 or earlier. It contains the following topics:

Adaptive Security Appliance and the ASA 5500 AIP SSM

The adaptive security appliance diverts packets to ASA 5500 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 ASA 5500 AIP SSM.

You can configure ASA 5500 AIP SSM to inspect traffic in inline or promiscuous mode and in fail-open or fail-over mode. You can use the adaptive security appliance CLI or ASDM to configure IPS traffic inspection.

Perform these steps on the adaptive security appliance to identify traffic to be diverted to and inspected by ASA 5500 AIP SSM:

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

Configuring the Adaptive Security Appliance to Send IPS Traffic to the ASA 5500 AIP SSM

To send traffic from the adaptive security appliance to ASA 5500 AIP SSM for the IPS to inspect, follow these steps:

Step 1 Log in to the adaptive security appliance.

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 an IPS class map to identify the traffic you want to send to ASA 5500 AIP SSM.

```
asa(config)# class-map class_map_name
```

Example

```
asa(config)# class-map ips_class
```

Note You can create multiple traffic class maps to send multiple traffic classes to ASA 5500 AIP SSM.

Step 5 Specify the traffic in the class map.

```
asa(config-cmap)# match parameter
```

Example

```
asa(config-cmap)# match [access-list | any]
```

Step 6 Add an IPS policy map that sets the actions to take with the class map traffic.

```
asa(config-cmap)# policy-map policy_map_name
```

Example

```
asa(config-cmap)# policy-map ips_policy
```

Step 7 Identify the class map you created in Step 4.

```
asa(config-pmap)# class class_map_name
```

Example

```
asa(config-pmap)# class ips_class
```

Step 8 Assign traffic to ASA 5500 AIP SSM.

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

Example

```
asa(config-pmap-c)# ips promiscuous fail-close
```

Step 9 (Optional) If you created multiple traffic class maps for IPS traffic, you can specify another class.

```
asa(config-pmap)# class class_map_name_2
```

Example

```
asa(config-pmap)# class ips_class_2
```

Step 10 (Optional) Specify the second class of traffic to send to ASA 5500 AIP SSM.

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

Example

```
asa(config-pmap-c)# ips promiscuous fail-close
```

Step 11 Activate the IPS service policy map on one or more interfaces.

```
asa(config)# service-policy policymap_name {global | interface interface_name}
```

Example

```
asa(config)# service-policy tcp_bypass_policy outside
```

Step 12 Verify the settings.

```
asa# show running-config
```

Step 13 Exit and save the configuration.

For More Information

For more information on bypass mode, see The Adaptive Security Appliance, ASA 5500 AIP SSM, and Bypass Mode, page 18-12.

The Adaptive Security Appliance, ASA 5500 AIP SSM, and Bypass Mode

The following conditions apply to bypass mode configuration, the adaptive security appliance, and the ASA 5500 AIP SSM.

The SensorApp Fails OR a Configuration Update is Taking Place

The following occurs when bypass is set to Auto or Off on the ASA IPS module:

- Bypass Auto—Traffic passes without inspection.
- Bypass Off—If the adaptive security appliance is configured for failover, then the adaptive security appliance fails over.

  If the adaptive security appliance is not configured for failover or failover is not possible:

  - If set to fail-open, the adaptive security appliance passes traffic without sending it to the ASA IPS module.
  - If set to fail-close, the adaptive security appliance stops passing traffic until the ASA IPS module is restarted or completes reconfiguration.

Note When bypass is set to On, traffic passes without inspection regardless of the state of the SensorApp.

The ASA 5500 AIP SSM Is Rebooted or Not Responding

The following occurs according to how the adaptive security appliance is configured for failover:

- If the adaptive security appliance is configured for failover, then the adaptive security appliance fails over.
- If the adaptive security appliance is not configured for failover or failover is not possible:
  - If set to fail-open, the adaptive security appliance passes traffic without sending it to the ASA IPS module.
  - If set to fail-close, the adaptive security appliance stops passing traffic until the ASA IPS module is restarted.

For More Information

For more information on bypass mode, see Configuring Inline Bypass Mode, page 5-38.

The ASA 5500 AIP SSM and the Normalizer Engine

The majority of the features in the Normalizer engine are not used on the ASA 5500 AIP SSM , because the ASA itself handles the normalization. Packets on the ASA IPS modules go through a special path in the Normalizer that only reassembles fragments and puts packets in the right order for the TCP stream. The Normalizer does not do any of the normalization that is done on an inline IPS appliance, because that causes problems in the way the ASA handles the packets.

The following Normalizer engine signatures are not supported:

- 1300.0
- 1304.0
- 1305.0
- 1307.0
- 1308.0
- 1309.0
- 1311.0
- 1315.0
- 1316.0
- 1317.0
- 1330.0
- 1330.1
- 1330.2
- 1330.9
- 1330.10
- 1330.12
- 1330.14
- 1330.15
- 1330.16
- 1330.17
- 1330.18

For More Information

For detailed information about the Normalizer engine, see Normalizer Engine, page B-37.

ASA 5500 AIP SSM Failover Scenarios

The following failover scenarios apply to the ASA in the event of configuration changes, signature/signature engine updates, service packs, and SensorApp crashes on the ASA 5500 AIP SSM.

Single ASA in Fail-Open Mode

- If the ASA is configured in fail-open mode for the ASA 5500 AIP SSM, and the ASA 5500 AIP SSM experiences a configuration change or signature/signature engine update, traffic is passed through the ASA without being inspected.
- If the ASA is configured in fail-open mode for the ASA 5500 AIP SSM, and the ASA 5500 AIP SSM experiences a SensorApp crash or a service pack upgrade, traffic is passed through the ASA without being inspected.

Single ASA in Fail-Close Mode

- If the ASA is configured in fail-close mode for the ASA 5500 AIP SSM, and the ASA 5500 AIP SSM experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the ASA.
- If the ASA is configured in fail-close mode for the ASA 5500 AIP SSM, and the ASA 5500 AIP SSM experiences a SensorApp crash or a service pack upgrade, traffic is stopped from passing through the ASA.

Two ASAs in Fail-Open Mode

- If the ASAs are configured in fail-open mode and if the ASA 5500 AIP SSM on the active ASA experiences a configuration change or a signature/signature engine update, traffic is still passed through the active ASA without being inspected. Failover is not triggered.
- If the ASAs are configured in fail-open mode, and if the ASA 5500 AIP SSM on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the ASA 5500 AIP SSM that was previously the standby module.

Two ASAs in Fail-Close Mode

- If the ASAs are configured in fail-close mode, and if the ASA 5500 AIP SSM on the active ASA experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the active ASA. No failover is triggered.
- If the ASAs are configured in fail-close mode, and if the ASA 5500 AIP SSM on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the module that was previously the standby for the ASA 5500 AIP SSM.

Configuration Examples

Use the following configuration for the primary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Use the following configuration for the secondary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit secondary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

The ASA 5500 AIP SSM and the Data Plane

Symptom The ASA 5500 AIP SSM data plane is kept in the Up state while applying signature updates. You can check the ASA 5500 AIP SSM data plane status by using the **show module** command during signature updates.

Possible Cause Bypass mode is set to off. The issue is seen when updating signatures, and when you use either CSM or IDM to apply signature updates. This issue is not seen when upgrading IPS system software.

The ASA 5500 AIP SSM and Jumbo Packets

The jumbo packet count in the **show interface** command output from the lines `Total Jumbo Packets Received` and `Total Jumbo Packets Transmitted` for ASA IPS modules may be larger than expected due to some packets that were almost jumbo size on the wire being counted as jumbo size by the IPS. This miscount is a result of header bytes added to the packet by the ASA before the packet is transmitted to the IPS. For IPv4, 58 bytes of header data are added. For IPv6, 78 bytes of header data are added. The ASA removes the added IPS header before the packet leaves the ASA.

Reloading, Shutting Down, Resetting, and Recovering the ASA 5500 AIP SSM

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 appliances 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).

Use the following commands to reload, shut down, reset, recover the password, and recover the ASA 5500 AIP SSM directly from the adaptive security appliance:

- **hw-module module** *slot_number* **reload—**This command reloads the software on the ASA 5500 AIP SSM without doing a hardware reset. It is effective only when the module is in the Up state.
- **hw-module module** *slot_number* **shutdown—**This command shuts down the software on the ASA 5500 AIP SSM. It is effective only when the module is in Up state.
- **hw-module module** *slot_number* **reset**—This command performs a hardware reset of the ASA 5500 AIP SSM. It is applicable when the module is in the Up/Down/Unresponsive/Recover states.
- **hw-module module** *slot_number* **password-reset—**This command restores the cisco CLI account password on the ASA 5500 AIP SSM to the default **cisco**.

- **hw-module module** *slot_number* **recover** [**boot** | **stop** | **configure**]—The **recover** command displays a set of interactive options for setting or changing the recovery parameters. To change the parameter or keep the existing setting, press **Enter**.
  - **hw-module module** *slot_number* **recover boot**—This command initiates recovery of the ASA 5500 AIP SSM. It is applicable only when the module is in the Up state.
  - **hw-module module** *slot_number* **recover stop**—This command stops recovery of the ASA 5500 AIP SSM. It is applicable only when the module is in the Recover state.

Caution If the ASA 5500 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 the recovery. Waiting any longer can lead to unexpected consequences. For example, the module may come up in the Unresponsive state.

  - **hw-module module 1 recover configure**—Use this command to configure parameters for the ASA 5500 AIP SSM recovery. The essential parameters are the IP address and recovery image TFTP URL location.

    Example

```
aip-ssm# hardware-module module 1 recover configure
Image URL [tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-7.1-1-E4.img]:
Port IP Address [10.89.149.226]:
VLAN ID [0]:
Gateway IP Address [10.89.149.254]:
```

For More Information

For the procedure for recovering the ASA 5500 AIP SSM system image, see Installing the System Image for the ASA 5500 AIP SSM, page 22-28.

New and Modified Commands

This section describes the new and modified Cisco ASA commands that support the ASA 5500 AIP SSM and are used to configure the ASA 5500 AIP SSM.

Note All other Cisco ASA CLI commands are documented in the *Cisco Security Appliance Command Reference* on Cisco.com at http://www.cisco.com/en/US/products/ps6120/prod_command_reference_list.html.

This section contains the following topic:

allocate-ips

To allocate an IPS virtual sensor to a security context if you have the ASA 5500 AIP SSM installed, use the **allocate-ips** command in context configuration mode. To remove a virtual sensor from a context, use the **no** form of this command.

allocate-ips *sensor_name* [*mapped_name*] [**default**]

no allocate-ips *sensor_name* [*mapped_name*] [**default**]

Syntax Description

default	(Optional) 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 ASA 5500 AIP SSM.
mapped_name	(Optional) Sets a mapped name 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” senors to sensor1 and sensor2 in context A, but map the “medsec” and “lowsec” sensors to sensor1 and sensor2 in context B.
sensor_name	Sets the sensor name configured on the ASA 5500 AIP SSM. To view the sensors that are configured on the ASA 5500 AIP SSM, 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 ASA 5500 AIP SSM, you get an error, but the **allocate-ips** command is entered as is. Until you create a sensor of that name on the ASA 5500 AIP SSM, the context assumes the sensor is down.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Context configuration	•	•	—	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can assign one or more IPS virtual sensors to each context. Then, when you configure the context to send traffic to the ASA 5500 AIP SSM using the **ips** command, 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 ASA 5500 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.

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 ASA 5500 AIP SSM 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
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
ips	Diverts traffic to the ASA 5500 AIP SSM for inspection.
show context	Shows a list of contexts (system execution space) or information about the current context.
show ips	Shows the virtual sensors configured on the ASA 5500 AIP SSM.