



Configuring the ASA 5500-X IPS SSP

This chapter contains procedures that are specific to configuring the ASA 5500-X IPS SSP. It contains the following sections:

- [Notes and Caveats for ASA 5500-X IPS SSP, page 19-1](#)
- [Configuration Sequence for the ASA 5500-X IPS SSP, page 19-2](#)
- [Verifying Initialization for the ASA 5500-X IPS SSP, page 19-3](#)
- [Creating Virtual Sensors for the ASA 5500-X IPS SSP, page 19-3](#)
- [TCP Reset Differences Between IPS Appliances and ASA IPS Modules, page 19-9](#)
- [Reloading IPS Messages, page 19-9](#)
- [ASA 5500-X IPS SSP Default Gateway, page 19-10](#)
- [Promiscuous Mode and Under Runs, page 19-10](#)
- [The ASA 5500-X IPS SSP and Bypass Mode, page 19-10](#)
- [The ASA 5500-X IPS SSP and the Normalizer Engine, page 19-11](#)
- [The ASA 5500-X IPS SSP and Memory Usage, page 19-12](#)
- [The ASA 5500-X IPS SSP and Jumbo Packets, page 19-12](#)
- [Reloading, Shutting Down, Resetting, and Recovering the ASA 5500-X IPS SSP, page 19-12](#)
- [Health and Status Information, page 19-13](#)
- [ASA 5500-X IPS SSP Failover Scenarios, page 19-15](#)
- [New and Modified Commands, page 19-16](#)

Notes and Caveats for ASA 5500-X IPS SSP

The following notes and caveats apply to configuring the ASA 5500-X IPS SSP:

- The ASA 5500-X IPS SSP is supported in ASA 8.6.1 and later.
- For the ASA 5500-X IPS SSP, normalization is performed by the adaptive security appliance and not the IPS.
- The ASA 5500-X IPS SSP does not support the inline TCP session tracking mode.
- The ASA 5500-X IPS SSP does not support CDP mode.
- Anomaly detection is disabled by default.

- All IPS platforms allow ten concurrent CLI sessions.
- The ASA 5500-X IPS SSP does not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the IPS.
- The ASA 5500-X IPS SSP (except the ASA 5512-X IPS SSP and the ASA 5515-X IPS SSP) support the String ICMP XL, String TCP XL, and String UDP XL engines. These engines provide optimized operation for these platforms.

Configuration Sequence for the ASA 5500-X IPS SSP

Perform the following tasks to configure the ASA 5500-X IPS SSP:

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-X IPS SSP.
4. Run the **setup** command to initialize the ASA 5500-X IPS SSP.
5. Verify initialization for the ASA 5500-X IPS SSP.
6. Configure the adaptive security appliance to send IPS traffic to the ASA 5500-X IPS SSP.
7. Perform other initial tasks, such as adding users, trusted hosts, and so forth.
8. Configure intrusion prevention.
9. Configure global correlation.
10. Configure global correlation.
11. Perform miscellaneous tasks to keep your ASA 5500-X IPS SSP running smoothly.
12. Upgrade the IPS software with new signature updates and service packs as they become available.
13. Reimage the ASA 5500-X IPS SSP when needed.

For More Information

- For the procedure for logging in to the ASA 5500-X IPS SSP, see [Chapter 2, “Logging In to the Sensor.”](#)
- For the procedure for running the **setup** command, see [Advanced Setup for the ASA 5500-X IPS SSP, page 3-18.](#)
- For the procedure for verifying initialization for the ASA 5500-X IPS SSP, see [Verifying Initialization for the ASA 5500-X IPS SSP, page 19-3.](#)
- For the procedure for creating virtual sensors, see [Creating Virtual Sensors for the ASA 5500-X IPS SSP, page 19-3.](#)
- For the procedures for setting up the ASA 5500-X IPS SSP, 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-X IPS SSP 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-X IPS SSP, see [Installing the System Image for the ASA 5500-X IPS SSP, page 22-31.](#)

Verifying Initialization for the ASA 5500-X IPS SSP

You can use the **show module slot details** command to verify that you have initialized the ASA 5500-X IPS SSP 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-X IPS SSP.

```
asa# show module ips details
Getting details from the Service Module, please wait...

Card Type:          ASA 5555-X IPS Security Services Processor
Model:              ASA5555-IPS
Hardware version:   N/A
Serial Number:      FCH151070GW
Firmware version:   N/A
Software version:   7.1(3)E4
MAC Address Range: 503d.e59c.7ca0 to 503d.e59c.7ca0
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(3)E4
Data Plane Status:  Up
Status:             Up
License:            IPS Module Enabled perpetual
Mgmt IP addr:       192.0.2.2
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   0.0.0.0/0
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

- Step 3** Confirm the information.
-

Creating Virtual Sensors for the ASA 5500-X IPS SSP

This section describes how to create virtual sensors on the ASA 5500-X IPS SSP, and contains the following topics:

- [The ASA 5500-X IPS SSP and Virtualization, page 19-4](#)
- [Virtual Sensor Configuration Sequence for ASA 5500-X IPS SSP, page 19-4](#)
- [Creating Virtual Sensors, page 19-4](#)
- [Assigning Virtual Sensors to Adaptive Security Appliance Contexts, page 19-6](#)

The ASA 5500-X IPS SSP and Virtualization

The ASA 5500-X IPS SSP has one sensing interface, PortChannel 0/0. 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.

Virtual Sensor Configuration Sequence for ASA 5500-X IPS SSP

Follow this sequence to create virtual sensors on the ASA 5500-X IPS SSP, and to assign them to adaptive security appliance contexts:

1. Configure up to four virtual sensors.
2. Assign the ASA 5500-X IPS SSP sensing interface (PortChannel 0/0) 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-X IPS SSP. 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, PortChannel 0/0 for the ASA 5500-X IPS SSP 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-X IPS SSP, 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 PortChannel10/0
```
- Step 9** Verify the virtual sensor settings.
- ```
sensor(config-ana-vir)# show settings
<protected entry>
name: vs1
-----
description: virtual sensor 1 default:
```

```

signature-definition: sig0 <protected>
event-action-rules: rules0 <protected>
anomaly-detection
-----
anomaly-detection-name: ad0 <protected>
operational-mode: inactive <defaulted>
-----
physical-interface (min: 0, max: 999999999, current: 1)
-----
name: PortChannel0/0
-----
inline-TCP-evasion-protection-mode: strict <defaulted>
-----
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 procedure for enabling anomaly detection, see [Enabling Anomaly Detection, page 9-8](#).
- 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-X IPS SSP, 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-X IPS SSP. 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-X IPS SSP, 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) #
```

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-X IPS SSP, 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-X IPS SSP 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-X IPS SSP Default Gateway

To access the Internet from the ASA 5500-X IPS SSP and to manage it from hosts behind other interfaces on the ASA 5500-X, connect the Management 0/0 interface on the ASA 5500-X to a Layer 3 device. Configure the default gateway on the sensor as the Layer 3 device. The appropriate static route on the ASA 5500-X is required so that the return traffic reaches the ASA 5500-X IPS SSP through this Layer 3 device.



Note

The Management 0/0 interface on the ASA 5500-X has no through traffic support. If the sensor is configured to use the IP address of the management interface of the ASA as the default gateway, the sensor cannot access the Internet and the sensor cannot be managed or accessed from the hosts behind the other interfaces on the ASA 5500-X.

Promiscuous Mode and Under Runs

The ASA 5500-X can exhibit under runs on the internal data interface going to the ASA 5500-X IPS SSP when it is configured in promiscuous mode.

The under runs for promiscuous mode inspection are expected behavior if you inspect a lot of traffic or have spikes in traffic rates, because the ASA does not wait for the ASA 5500-X IPS SSP to finish inspection before forwarding traffic. It is also possible to have under runs if the ASA 5500-X IPS SSP inspects long flows, such as file downloads. If you have a lot of long flows, you can limit IPS inspection with the **specify-flow-depth** setting under **service analysis-engine global-settings**. Limiting inspection to 800,000 bytes per stream reduces the number of under runs. You can check for symptoms of long flows by looking at the per CPU processing load percentage statistics in **show statistics analysis-engine**. If any of the threads are running at 100%, this may be triggered by a long flow.

For More Information

- For the procedure for specifying flow depth, see [Configuring Global Variables, page 6-12](#).
- For the procedure for checking the load percentage statistics, see [Displaying Statistics, page 17-31](#).

The ASA 5500-X IPS SSP and Bypass Mode

The ASA 5500-X IPS SSP does not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the ASA 5500-X IPS SSP.

The SensorApp Fails

The following occurs when the SensorApp fails:

- 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.

The SensorApp is Reconfigured

The following occurs when the SensorApp is reconfigured:

- 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.

**Note**

The adaptive security appliance does not failover unless the reconfiguration is not completed.

The ASA 5500-X IPS SSP and the Normalizer Engine

The majority of the features in the Normalizer engine are not used on the ASA 5500-X IPS SSP, 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](#).

The ASA 5500-X IPS SSP and Memory Usage

For the ASA 5500-X IPS SSP, the memory usage is 93%. The default health thresholds for the sensor are 80% for yellow and 91% for red, so the sensor health will be shown as red on these platforms even for normal operating conditions. You can tune the threshold percentage for memory usage so that it reads more accurately for these platforms by configuring the **memory-usage-policy** option in the sensor health metrics.

**Note**

Make sure you have the **memory-usage-policy** option in the sensor health metrics enabled.

[Table 19-1](#) lists the yellow-threshold and the red-threshold health values.

Table 19-1 ASA 5500-X IPS SSP Memory Usage Values

Platform	Yellow	Red	Memory Used
ASA 5512-X IPS SSP	85%	91%	28%
ASA 5515-X IPS SSP	88%	92%	14%
ASA 5525-X IPS SSP	88%	92%	14%
ASA 5545-X IPS SSP	93%	96%	13%
ASA 5555-X IPS SSP	95%	98%	17%

The ASA 5500-X IPS SSP 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-X IPS SSP

**Note**

You can enter the **sw-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 **sw-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-X IPS SSP directly from the adaptive security appliance:

- **sw-module module ips reload**—This command reloads the software on the ASA 5500-X IPS SSP without doing a hardware reset. It is effective only when the module is in the Up state.
- **sw-module module ips shutdown**—This command shuts down the software on the ASA 5500-X IPS SSP. It is effective only when the module is in Up state.
- **sw-module module ips reset**—This command performs a hardware reset of the ASA 5500-X IPS SSP. It is applicable when the module is in the Up/Down/Unresponsive/Recover states.
- **sw-module module ips password-reset**—This command restores the cisco CLI account password on the ASA 5500-X IPS SSP to the default **cisco**.
- **sw-module module ips recover image disk0:/image name**—This command starts the reimage process by setting the image location and name. You must first copy the IPS image to the ASA to disk0:/.
- **sw-module module ips recover boot**—This command reimages the ASA 5500-X IPS SSP. It is applicable only when the module is in the Up state.
- **sw-module module ips recover stop**—This command stops the reimage of the ASA 5500-X IPS SSP. It is applicable only when the module is in the Recover state.



Caution

If the ASA 5500-X IPS SSP recovery needs to be stopped, you must issue the **sw-module module ips 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.

- **sw-module module ips recover configure**—Use this command to configure parameters for the ASA 5500-X IPS SSP recovery. The essential parameters are the IP address and recovery image TFTP URL location.

Example

```
asa-ips# sw-module module ips recover configure image
disk0:/IPS-SSP_5555-K9-sys-1.1-a-7.1-3-E4.aip
Image URL [tftp://192.0.2.1/IPS-5545-K9-sys-1.1-a-7.1-3-E4.aip]:
Port IP Address [192.0.2.226]:
VLAN ID [0]:
Gateway IP Address [192.0.2.254]:
```

For More Information

For the procedure for recovering the ASA 5500-X IPS SSP system image, see [Installing the System Image for the ASA 5500-X IPS SSP](#), page 22-31.

Health and Status Information

To see the general health of the ASA 5500-X IPS SSP, use the **show module ips details** command.

```
asa# show module ips details
Getting details from the Service Module, please wait...

Card Type:           IPS 5555 Intrusion Prevention System
Model:               IPS5555
Hardware version:    N/A
Serial Number:       FCH1504V0CW
```

```

Firmware version:  N/A
Software version:  7.1(3)E4
MAC Address Range: 503d.e59c.7ca0 to 503d.e59c.7ca0
App. name:         IPS
App. Status:       Up
App. Status Desc:  Normal Operation
App. version:      7.1(3)E4
Data Plane Status: Up
Status:            Up
License:           IPS Module Enabled perpetual
Mgmt IP addr:      192.168.1.2
Mgmt Network mask: 255.255.255.0
Mgmt Gateway:      192.168.1.1
Mgmt web ports:    443
Mgmt TLS enabled:  true
asa#

```

The output shows that the ASA 5500-X IPS SSP is up. If the status reads *Down*, you can reset it using the **sw-module module 1 reset** command.

If you have problems with reimaging the ASA 5500-X IPS SSP, use the **debug module-boot** command to see the output as it boots. Make sure you have the correct IP address for the TFTP server and you have the correct file on the TFTP server. Then use the **sw-module module ips recover** command again to reimage the module.

```

asa-ips# sw-module module ips recover configure image
disk0:/IPS-SSP_5555-K9-sys-1.1-a-7.1-3-E4.aip
Image URL [tftp://192.0.2.1/IPS-5545-K9-sys-1.1-a-7.1-3-E4.aip]:
Port IP Address [192.0.2.226]:
VLAN ID [0]:
Gateway IP Address [192.0.2.254]:

asa-ips# debug module-boot
debug module-boot  enabled at level 1
asa-ips# sw-module module ips reload

Reload module ips? [confirm]
Reload issued for module ips.
asa-ips# Mod-ips 228> ***
Mod-ips 229> *** EVENT: The module is reloading.
Mod-ips 230> *** TIME: 08:07:36 CST Jan 17 2012
Mod-ips 231> ***
Mod-ips 232> Mod-ips 233> The system is going down NOW!
Mod-ips 234> Sending SIGTERM to all processes
Mod-ips 235> Sending SIGKILL to all processes
Mod-ips 236> Requesting system reboot
Mod-ips 237> e1000 0000:00:07.0: PCI INT A disabled
Mod-ips 238> e1000 0000:00:06.0: PCI INT A disabled
Mod-ips 239> e1000 0000:00:05.0: PCI INT A disabled
Mod-ips 240> Restarting system.
Mod-ips 241> machine restart
Mod-ips 242> IVSHMEM: addr = 4093640704 size = 67108864
Mod-ips 243> Booting 'Cisco IPS'
-MORE-

```

ASA 5500-X IPS SSP Failover Scenarios

The following failover scenarios apply to the ASA 5500-X series in the event of configuration changes, signature/signature engine updates, service packs, and SensorApp crashes on the ASA 5500-X IPS SSP.

Single ASA in Fail-Open Mode

- If the ASA is configured in fail-open mode for the ASA 5500-X IPS SSP, and the ASA 5500-X IPS SSP 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-X IPS SSP, and the ASA 5500-X IPS SSP 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-X IPS SSP, and the ASA 5500-X IPS SSP 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-X IPS SSP, and the ASA 5500-X IPS SSP 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-X IPS SSP 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-X IPS SSP on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the ASA 5500-X IPS SSP that was previously the standby ASA 5500-X IPS SSP.

Two ASAs in Fail-Close Mode

- If the ASAs are configured in fail-close mode, and if the ASA 5500-X IPS SSP 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-X IPS SSP on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the ASA 5500-X IPS SSP that was previously the standby for the ASA 5500-X IPS SSP.

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

```

New and Modified Commands

This section describes the new and modified Cisco ASA commands that support the ASA 5500-X IPS SSP and are used to configure the ASA 5500-X IPS SSP.



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, page 19-16](#)

allocate-ips

To allocate an IPS virtual sensor to a security context if you have the ASA 5500-X IPS SSP 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-X IPS SSP.
----------------	--

<i>mapped_name</i>	(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” sensors to sensor1 and sensor2 in context A, but map the “medsec” and “lowsec” sensors to sensor1 and sensor2 in context B.
<i>sensor_name</i>	Sets the sensor name configured on the ASA 5500-X IPS SSP. To view the sensors that are configured on the ASA 5500-X IPS SSP, 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-X IPS SSP, 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-X IPS SSP, 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple 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-X IPS SSP 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-X IPS SSP 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-X IPS SSP 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-X IPS SSP 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-X IPS SSP.