CHAPTER 18

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 18-1
- Configuration Sequence for the ASA 5500-X IPS SSP, page 18-2
- Verifying Initialization for the ASA 5500-X IPS SSP, page 18-3
- Creating Virtual Sensors for the ASA 5500-X IPS SSP, page 18-3
- The ASA 5500-X IPS SSP and Bypass Mode, page 18-9
- The ASA 5500-X IPS SSP and the Normalizer Engine, page 18-9
- The ASA 5500-X IPS SSP and Memory Usage, page 18-11
- The ASA 5500-X IPS SSP and Jumbo Packets, page 18-10
- TCP Reset Differences Between IPS Appliances and the ASA 5500-X IPS SSP, page 18-11
- Reloading IPS Messages, page 18-11
- Reloading, Shutting Down, Resetting, and Recovering the ASA 5500-X IPS SSP, page 18-12
- Health and Status Information, page 18-13
- ASA 5500-X IPS SSP Failover Scenarios, page 18-20
- New and Modified Commands, page 18-21

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) supports 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. Perform miscellaneous tasks to keep your ASA 5500-X IPS SSP running smoothly.
11. Upgrade the IPS software with new signature updates and service packs as they become available.
12. 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 3-14.
- For the procedure for verifying initialization for the ASA 5500-X IPS SSP, see Verifying Initialization for the ASA 5500-X IPS SSP, page 18-3.
- For the procedure for creating virtual sensors, see Creating Virtual Sensors for the ASA 5500-X IPS SSP, page 18-3.
- 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 8, “Configuring Event Action Rules,” Chapter 7, “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 20, "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 21-22.

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 SSPS.

```
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:   7.2(1)E4
MAC Address Range:  503d.e59c.7ca0 to 503d.e59c.7ca0
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2(1)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 18-4
- Virtual Sensor Configuration Sequence for ASA 5500-X IPS SSP, page 18-4
- Creating Virtual Sensors, page 18-4
- Assigning Virtual Sensors to Adaptive Security Appliance Contexts, page 18-6

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 parameters 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. 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 PortChannel0/0
```

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

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 parameters 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)#
```

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 fail over 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-36.

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.

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 18-1 lists the yellow-threshold and the red-threshold health values.

Table 18-1 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%

TCP Reset Differences Between IPS Appliances and the ASA 5500-X IPS SSP

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.

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-7.2-1-E4.aip
Image URL [tftp://192.0.2.1/IPS-5545-K9-sys-1.1-a-7.2-1-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 21-22.

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:   7.2(1)E4
MAC Address Range:  503d.e59c.7ca0 to 503d.e59c.7ca0
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2(1)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-7.2-1-E4.aip
Image URL [tftp://192.0.2.1/IPS-5545-K9-sys-1.1-a-7.2-1-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'
Mod-ips 244> root (hd0,0)
Mod-ips 245>  Filesystem type is ext2fs, partition type 0x83
Mod-ips 246> kernel /ips-2.6.ld ro initfsDev=/dev/hda1 init=loader.run rootrw=/dev/hda2
init
Mod-ips 247> fs=runtime-image.cpio.bz2 hda=nodma console=ttyS0 plat=saleen htlblow=1
hugepag
Mod-ips 248> es=3223
Mod-ips 249>    [Linux-bzImage, setup=0x2c00, size=0x2bad80]
Mod-ips 250> Linux version 2.6.29.1 (ipsbuild@seti-teambuilder-a) (gcc version 4.3.2
(crosstool
Mod-ips 251> -NG-1.4.1) ) #56 SMP Tue Dec 6 00:46:11 CST 2011
Mod-ips 252> Command line: ro initfsDev=/dev/hda1 init=loader.run rootrw=/dev/hda2
initfs=runti
Mod-ips 253> me-image.cpio.bz2 hda=nodma console=ttyS0 plat=saleen htlblow=1
hugepages=3223
Mod-ips 254> KERNEL supported cpus:
Mod-ips 255>   Intel GenuineIntel
Mod-ips 256>   AMD AuthenticAMD
Mod-ips 257>   Centaur CentaurHauls
Mod-ips 258> BIOS-provided physical RAM map:
Mod-ips 259>  BIOS-e820: 0000000000000000 - 000000000009f400 (usable)
Mod-ips 260>  BIOS-e820: 000000000009f400 - 00000000000a0000 (reserved)
Mod-ips 261>  BIOS-e820: 00000000000f0000 - 0000000000100000 (reserved)
Mod-ips 262>  BIOS-e820: 0000000000100000 - 00000000dfffd000 (usable)
Mod-ips 263>  BIOS-e820: 00000000dfffd000 - 00000000e0000000 (reserved)
Mod-ips 264>  BIOS-e820: 00000000fffbc000 - 0000000100000000 (reserved)
Mod-ips 265>  BIOS-e820: 0000000100000000 - 0000000201400000 (usable)
Mod-ips 266> DMI 2.4 present.
Mod-ips 267> last_pfn = 0x201400 max_arch_pfn = 0x100000000
Mod-ips 268> last_pfn = 0xdfffd max_arch_pfn = 0x100000000
Mod-ips 269> init_memory_mapping: 0000000000000000-00000000dfffd000
Mod-ips 270> last_map_addr: dfffd000 end: dfffd000
Mod-ips 271> init_memory_mapping: 0000000100000000-0000000201400000
Mod-ips 272> last_map_addr: 201400000 end: 201400000
Mod-ips 273> ACPI: RSDP 000F88D0, 0014 (r0 BOCHS )
Mod-ips 274> ACPI: RSDT DFFFDD00, 0034 (r1 BOCHS  BXPCRSDT        1 BXPC        1)
Mod-ips 275> ACPI: FACP DFFFFD90, 0074 (r1 BOCHS  BXPCFACP        1 BXPC        1)
Mod-ips 276> FADT: X_PM1a_EVT_BLK.bit_width (16) does not match PM1_EVT_LEN (4)
Mod-ips 277> ACPI: DSDT DFFFDF10, 1E22 (r1   BXPC   BXDSDT        1 INTL 20090123)
Mod-ips 278> ACPI: FACS DFFFFD40, 0040
Mod-ips 279> ACPI: SSDT DFFFDE90, 0079 (r1 BOCHS  BXPCSSDT        1 BXPC        1)
Mod-ips 280> ACPI: APIC DFFFDD80, 0090 (r1 BOCHS  BXPCAPIC        1 BXPC        1)
Mod-ips 281> ACPI: HPET DFFFDD40, 0038 (r1 BOCHS  BXPCHPET        1 BXPC        1)
Mod-ips 282> No NUMA configuration found
Mod-ips 283> Faking a node at 0000000000000000-0000000201400000
Mod-ips 284> Bootmem setup node 0 0000000000000000-0000000201400000
Mod-ips 285>   NODE_DATA [0000000000011000 - 000000000001ffff]
Mod-ips 286>   bootmap [0000000000020000 -  000000000006027f] pages 41
Mod-ips 287> (6 early reservations) ==> bootmem [0000000000 - 0201400000]
Mod-ips 288>   #0 [0000000000 - 0000001000]   BIOS data page ==> [0000000000 - 0000001000]
Mod-ips 289>   #1 [0000006000 - 0000008000]       TRAMPOLINE ==> [0000006000 - 0000008000]
Mod-ips 290>   #2 [0000200000 - 0000d55754]    TEXT DATA BSS ==> [0000200000 - 0000d55754]
```

```
Mod-ips 291>   #3 [000009f400 - 0000100000]    BIOS reserved ==> [000009f400 - 0000100000]
Mod-ips 292>   #4 [0000008000 - 000000c000]          PGTABLE ==> [0000008000 - 000000c000]
Mod-ips 293>   #5 [000000c000 - 0000011000]          PGTABLE ==> [000000c000 - 0000011000]
Mod-ips 294> found SMP MP-table at [ffff8800000f8920] 000f8920
Mod-ips 295> Zone PFN ranges:
Mod-ips 296>   DMA      0x00000000 -> 0x00001000
Mod-ips 297>   DMA32    0x00001000 -> 0x00100000
Mod-ips 298>   Normal   0x00100000 -> 0x00201400
Mod-ips 299> Movable zone start PFN for each node
Mod-ips 300> early_node_map[3] active PFN ranges
Mod-ips 301>     0: 0x00000000 -> 0x0000009f
Mod-ips 302>     0: 0x00000100 -> 0x000dfffd
Mod-ips 303>     0: 0x00100000 -> 0x00201400
Mod-ips 304> ACPI: PM-Timer IO Port: 0xb008
Mod-ips 305> ACPI: LAPIC (acpi_id[0x00] lapic_id[0x00] enabled)
Mod-ips 306> ACPI: LAPIC (acpi_id[0x01] lapic_id[0x01] enabled)
Mod-ips 307> ACPI: LAPIC (acpi_id[0x02] lapic_id[0x02] enabled)
Mod-ips 308> ACPI: LAPIC (acpi_id[0x03] lapic_id[0x03] enabled)
Mod-ips 309> ACPI: LAPIC (acpi_id[0x04] lapic_id[0x04] enabled)
Mod-ips 310> ACPI: LAPIC (acpi_id[0x05] lapic_id[0x05] enabled)
Mod-ips 311> ACPI: IOAPIC (id[0x06] address[0xfec00000] gsi_base[0])
Mod-ips 312> IOAPIC[0]: apic_id 6, version 0, address 0xfec00000, GSI 0-23
Mod-ips 313> ACPI: INT_SRC_OVR (bus 0 bus_irq 5 global_irq 5 high level)
Mod-ips 314> ACPI: INT_SRC_OVR (bus 0 bus_irq 9 global_irq 9 high level)
Mod-ips 315> ACPI: INT_SRC_OVR (bus 0 bus_irq 10 global_irq 10 high level)
Mod-ips 316> ACPI: INT_SRC_OVR (bus 0 bus_irq 11 global_irq 11 high level)
Mod-ips 317> Using ACPI (MADT) for SMP configuration information
Mod-ips 318> ACPI: HPET id: 0x8086a201 base: 0xfed00000
Mod-ips 319> SMP: Allowing 6 CPUs, 0 hotplug CPUs
Mod-ips 320> Allocating PCI resources starting at e2000000 (gap: e0000000:1ffbc000)
Mod-ips 321> NR_CPUS:32 nr_cpumask_bits:32 nr_cpu_ids:6 nr_node_ids:1
Mod-ips 322> PERCPU: Allocating 49152 bytes of per cpu data
Mod-ips 323> Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 1939347
Mod-ips 324> Policy zone: Normal
Mod-ips 325> Kernel command line: ro initfsDev=/dev/hda1 init=loader.run rootrw=/dev/hda2
initf
Mod-ips 326> s=runtime-image.cpio.bz2 hda=nodma console=ttyS0 plat=saleen htlblow=1
hugepages=3
Mod-ips 327> 223
Mod-ips 328> hugetlb_lowmem_setup: Allocated 2097152 huge pages (size=0x200000) from
lowmem are
Mod-ips 329> a at 0xffff88002ee00000 phys addr 0x000000002ee00000
Mod-ips 330> Initializing CPU#0
Mod-ips 331> PID hash table entries: 4096 (order: 12, 32768 bytes)
Mod-ips 332> Fast TSC calibration using PIT
Mod-ips 333> Detected 2792.965 MHz processor.
Mod-ips 334> Console: colour VGA+ 80x25
Mod-ips 335> console [ttyS0] enabled
Mod-ips 336> Checking aperture...
Mod-ips 337> No AGP bridge found
Mod-ips 338> PCI-DMA: Using software bounce buffering for IO (SWIOTLB)
Mod-ips 339> Placing 64MB software IO TLB between ffff880020000000 - ffff880024000000
Mod-ips 340> software IO TLB at phys 0x20000000 - 0x24000000
Mod-ips 341> Memory: 7693472k/8409088k available (3164k kernel code, 524688k absent,
190928k re
Mod-ips 342> served, 1511k data, 1032k init)
Mod-ips 343> Calibrating delay loop (skipped), value calculated using timer frequency..
5585.93
Mod-ips 344>  BogoMIPS (lpj=2792965)
Mod-ips 345> Dentry cache hash table entries: 1048576 (order: 11, 8388608 bytes)
Mod-ips 346> Inode-cache hash table entries: 524288 (order: 10, 4194304 bytes)
Mod-ips 347> Mount-cache hash table entries: 256
Mod-ips 348> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 349> CPU: L2 cache: 4096K
```

```
Mod-ips 350> CPU 0/0x0 -> Node 0
Mod-ips 351> Freeing SMP alternatives: 29k freed
Mod-ips 352> ACPI: Core revision 20081204
Mod-ips 353> Setting APIC routing to flat
Mod-ips 354> ..TIMER: vector=0x30 apic1=0 pin1=0 apic2=-1 pin2=-1
Mod-ips 355> CPU0: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 356> Booting processor 1 APIC 0x1 ip 0x6000
Mod-ips 357> Initializing CPU#1
Mod-ips 358> Calibrating delay using timer specific routine.. 5585.16 BogoMIPS
(lpj=2792581)
Mod-ips 359> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 360> CPU: L2 cache: 4096K
Mod-ips 361> CPU 1/0x1 -> Node 0
Mod-ips 362> CPU1: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 363> checking TSC synchronization [CPU#0 -> CPU#1]:
Mod-ips 364> Measured 1453783140569731 cycles TSC warp between CPUs, turning off TSC
clock.
Mod-ips 365> Marking TSC unstable due to check_tsc_sync_source failed
Mod-ips 366> Booting processor 2 APIC 0x2 ip 0x6000
Mod-ips 367> Initializing CPU#2
Mod-ips 368> Calibrating delay using timer specific routine.. 5580.51 BogoMIPS
(lpj=2790259)
Mod-ips 369> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 370> CPU: L2 cache: 4096K
Mod-ips 371> CPU 2/0x2 -> Node 0
Mod-ips 372> CPU2: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 373> Booting processor 3 APIC 0x3 ip 0x6000
Mod-ips 374> Initializing CPU#3
Mod-ips 375> Calibrating delay using timer specific routine.. 5585.18 BogoMIPS
(lpj=2792594)
Mod-ips 376> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 377> CPU: L2 cache: 4096K
Mod-ips 378> CPU 3/0x3 -> Node 0
Mod-ips 379> CPU3: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 380> Booting processor 4 APIC 0x4 ip 0x6000
Mod-ips 381> Initializing CPU#4
Mod-ips 382> Calibrating delay using timer specific routine.. 5585.15 BogoMIPS
(lpj=2792579)
Mod-ips 383> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 384> CPU: L2 cache: 4096K
Mod-ips 385> CPU 4/0x4 -> Node 0
Mod-ips 386> CPU4: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 387> Booting processor 5 APIC 0x5 ip 0x6000
Mod-ips 388> Initializing CPU#5
Mod-ips 389> Calibrating delay using timer specific routine.. 5585.21 BogoMIPS
(lpj=2792609)
Mod-ips 390> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 391> CPU: L2 cache: 4096K
Mod-ips 392> CPU 5/0x5 -> Node 0
Mod-ips 393> CPU5: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 394> Brought up 6 CPUs
Mod-ips 395> Total of 6 processors activated (33507.17 BogoMIPS).
Mod-ips 396> net_namespace: 1312 bytes
Mod-ips 397> Booting paravirtualized kernel on bare hardware
Mod-ips 398> NET: Registered protocol family 16
Mod-ips 399> ACPI: bus type pci registered
Mod-ips 400> dca service started, version 1.8
Mod-ips 401> PCI: Using configuration type 1 for base access
Mod-ips 402> mtrr: your CPUs had inconsistent variable MTRR settings
Mod-ips 403> mtrr: your CPUs had inconsistent MTRRdefType settings
Mod-ips 404> mtrr: probably your BIOS does not setup all CPUs.
Mod-ips 405> mtrr: corrected configuration.
Mod-ips 406> bio: create slab <bio-0> at 0
Mod-ips 407> ACPI: Interpreter enabled
```

```
Mod-ips 408> ACPI: (supports S0 S5)
Mod-ips 409> ACPI: Using IOAPIC for interrupt routing
Mod-ips 410> ACPI: No dock devices found.
Mod-ips 411> ACPI: PCI Root Bridge [PCI0] (0000:00)
Mod-ips 412> pci 0000:00:01.3: quirk: region b000-b03f claimed by PIIX4 ACPI
Mod-ips 413> pci 0000:00:01.3: quirk: region b100-b10f claimed by PIIX4 SMB
Mod-ips 414> IVSHMEM: addr = 4093640704 size = 67108864
Mod-ips 415> ACPI: PCI Interrupt Link [LNKA] (IRQs 5 *10 11)
Mod-ips 416> ACPI: PCI Interrupt Link [LNKB] (IRQs 5 *10 11)
Mod-ips 417> ACPI: PCI Interrupt Link [LNKC] (IRQs 5 10 *11)
Mod-ips 418> ACPI: PCI Interrupt Link [LNKD] (IRQs 5 10 *11)
Mod-ips 419> SCSI subsystem initialized
Mod-ips 420> usbcore: registered new interface driver usbfs
Mod-ips 421> usbcore: registered new interface driver hub
Mod-ips 422> usbcore: registered new device driver usb
Mod-ips 423> PCI: Using ACPI for IRQ routing
Mod-ips 424> pnp: PnP ACPI init
Mod-ips 425> ACPI: bus type pnp registered
Mod-ips 426> pnp: PnP ACPI: found 9 devices
Mod-ips 427> ACPI: ACPI bus type pnp unregistered
Mod-ips 428> NET: Registered protocol family 2
Mod-ips 429> IP route cache hash table entries: 262144 (order: 9, 2097152 bytes)
Mod-ips 430> TCP established hash table entries: 524288 (order: 11, 8388608 bytes)
Mod-ips 431> TCP bind hash table entries: 65536 (order: 8, 1048576 bytes)
Mod-ips 432> TCP: Hash tables configured (established 524288 bind 65536)
Mod-ips 433> TCP reno registered
Mod-ips 434> NET: Registered protocol family 1
Mod-ips 435> Adding htlb page ffff88002ee00000 phys 000000002ee00000 page ffffe20000a41000
Mod-ips 436> HugeTLB registered 2 MB page size, pre-allocated 3223 pages
Mod-ips 437> report_hugepages: Using 1 pages from low memory at ffff88002ee00000 HugeTLB
FS
Mod-ips 438> msgmni has been set to 15026
Mod-ips 439> alg: No test for stdrng (krng)
Mod-ips 440> io scheduler noop registered
Mod-ips 441> io scheduler anticipatory registered
Mod-ips 442> io scheduler deadline registered
Mod-ips 443> io scheduler cfq registered (default)
Mod-ips 444> pci 0000:00:00.0: Limiting direct PCI/PCI transfers
Mod-ips 445> pci 0000:00:01.0: PIIX3: Enabling Passive Release
Mod-ips 446> pci 0000:00:01.0: Activating ISA DMA hang workarounds
Mod-ips 447> pci_hotplug: PCI Hot Plug PCI Core version: 0.5
Mod-ips 448> pciehp: PCI Express Hot Plug Controller Driver version: 0.4
Mod-ips 449> acpiphp: ACPI Hot Plug PCI Controller Driver version: 0.5
Mod-ips 450> acpiphp_glue: can't get bus number, assuming 0
Mod-ips 451> decode_hpp: Could not get hotplug parameters. Use defaults
Mod-ips 452> acpiphp: Slot [1] registered
Mod-ips 453> acpiphp: Slot [2] registered
Mod-ips 454> acpiphp: Slot [3] registered
Mod-ips 455> acpiphp: Slot [4] registered
Mod-ips 456> acpiphp: Slot [5] registered
Mod-ips 457> acpiphp: Slot [6] registered
Mod-ips 458> acpiphp: Slot [7] registered
Mod-ips 459> acpiphp: Slot [8] registered
Mod-ips 460> acpiphp: Slot [9] registered
Mod-ips 461> acpiphp: Slot [10] registered
Mod-ips 462> acpiphp: Slot [11] registered
Mod-ips 463> acpiphp: Slot [12] registered
Mod-ips 464> acpiphp: Slot [13] registered
Mod-ips 465> acpiphp: Slot [14] registered
Mod-ips 466> acpiphp: Slot [15] registered
Mod-ips 467> acpiphp: Slot [16] registered
Mod-ips 468> acpiphp: Slot [17] registered
Mod-ips 469> acpiphp: Slot [18] registered
Mod-ips 470> acpiphp: Slot [19] registered
```

```
Mod-ips 471> acpiphp: Slot [20] registered
Mod-ips 472> acpiphp: Slot [21] registered
Mod-ips 473> acpiphp: Slot [22] registered
Mod-ips 474> acpiphp: Slot [23] registered
Mod-ips 475> acpiphp: Slot [24] registered
Mod-ips 476> acpiphp: Slot [25] registered
Mod-ips 477> acpiphp: Slot [26] registered
Mod-ips 478> acpiphp: Slot [27] registered
Mod-ips 479> acpiphp: Slot [28] registered
Mod-ips 480> acpiphp: Slot [29] registered
Mod-ips 481> acpiphp: Slot [30] registered
Mod-ips 482> acpiphp: Slot [31] registered
Mod-ips 483> shpchp: Standard Hot Plug PCI Controller Driver version: 0.4
Mod-ips 484> fakephp: Fake PCI Hot Plug Controller Driver
Mod-ips 485> fakephp: pci_hp_register failed with error -16
Mod-ips 486> fakephp: pci_hp_register failed with error -16
Mod-ips 487> fakephp: pci_hp_register failed with error -16
Mod-ips 488> fakephp: pci_hp_register failed with error -16
Mod-ips 489> fakephp: pci_hp_register failed with error -16
Mod-ips 490> fakephp: pci_hp_register failed with error -16
Mod-ips 491> fakephp: pci_hp_register failed with error -16
Mod-ips 492> processor ACPI_CPU:00: registered as cooling_device0
Mod-ips 493> processor ACPI_CPU:01: registered as cooling_device1
Mod-ips 494> processor ACPI_CPU:02: registered as cooling_device2
Mod-ips 495> processor ACPI_CPU:03: registered as cooling_device3
Mod-ips 496> processor ACPI_CPU:04: registered as cooling_device4
Mod-ips 497> processor ACPI_CPU:05: registered as cooling_device5
Mod-ips 498> hpet_acpi_add: no address or irqs in _CRS
Mod-ips 499> Non-volatile memory driver v1.3
Mod-ips 500> Linux agpgart interface v0.103
Mod-ips 501> ipmi message handler version 39.2
Mod-ips 502> ipmi device interface
Mod-ips 503> IPMI System Interface driver.
Mod-ips 504> ipmi_si: Unable to find any System Interface(s)
Mod-ips 505> IPMI SMB Interface driver
Mod-ips 506> IPMI Watchdog: driver initialized
Mod-ips 507> Copyright (C) 2004 MontaVista Software - IPMI Powerdown via sys_reboot.
Mod-ips 508> Serial: 8250/16550 driver, 4 ports, IRQ sharing enabled
Mod-ips 509> ?serial8250: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
Mod-ips 510> serial8250: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
Mod-ips 511> 00:06: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
Mod-ips 512> 00:07: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
Mod-ips 513> brd: module loaded
Mod-ips 514> loop: module loaded
Mod-ips 515> lpc: version 0.1 (Nov 10 2011)
Mod-ips 516> tun: Universal TUN/TAP device driver, 1.6
Mod-ips 517> tun: (C) 1999-2004 Max Krasnyansky <maxk@qualcomm.com>
Mod-ips 518> Uniform Multi-Platform E-IDE driver
Mod-ips 519> piix 0000:00:01.1: IDE controller (0x8086:0x7010 rev 0x00)
Mod-ips 520> piix 0000:00:01.1: not 100native mode: will probe irqs later
Mod-ips 521>     ide0: BM-DMA at 0xc000-0xc007
Mod-ips 522>     ide1: BM-DMA at 0xc008-0xc00f
Mod-ips 523> hda: QEMU HARDDISK, ATA DISK drive
Mod-ips 524> Clocksource tsc unstable (delta = 2851415955127 ns)
Mod-ips 525> hda: MWDMA2 mode selected
Mod-ips 526> hdc: QEMU DVD-ROM, ATAPI CD/DVD-ROM drive
Mod-ips 527> hdc: MWDMA2 mode selected
Mod-ips 528> ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
Mod-ips 529> ide1 at 0x170-0x177,0x376 on irq 15
Mod-ips 530> ide_generic: please use "probe_mask=0x3f" module parameter for probing all
legacy
Mod-ips 531> ISA IDE ports
Mod-ips 532> ide-gd driver 1.18
Mod-ips 533> hda: max request size: 512KiB
```

```
Mod-ips 534> hda: 7815168 sectors (4001 MB) w/256KiB Cache, CHS=7753/255/63
Mod-ips 535> hda: cache flushes supported
Mod-ips 536>  hda: hda1 hda2 hda3 hda4
Mod-ips 537> Driver 'sd' needs updating - please use bus_type methods
Mod-ips 538> Driver 'sr' needs updating - please use bus_type methods
Mod-ips 539> ehci_hcd: USB 2.0 'Enhanced' Host Controller (EHCI) Driver
Mod-ips 540> ohci_hcd: USB 1.1 'Open' Host Controller (OHCI) Driver
Mod-ips 541> uhci_hcd: USB Universal Host Controller Interface driver
Mod-ips 542> Initializing USB Mass Storage driver...
Mod-ips 543> usbcore: registered new interface driver usb-storage
Mod-ips 544> USB Mass Storage support registered.
Mod-ips 545> PNP: PS/2 Controller [PNP0303:KBD,PNP0f13:MOU] at 0x60,0x64 irq 1,12
Mod-ips 546> serio: i8042 KBD port at 0x60,0x64 irq 1
Mod-ips 547> serio: i8042 AUX port at 0x60,0x64 irq 12
Mod-ips 548> mice: PS/2 mouse device common for all mice
Mod-ips 549> rtc_cmos 00:01: rtc core: registered rtc_cmos as rtc0
Mod-ips 550> rtc0: alarms up to one day, 114 bytes nvram
Mod-ips 551> input: AT Translated Set 2 keyboard as /class/input/input0
Mod-ips 552> i2c /dev entries driver
Mod-ips 553> piix4_smbus 0000:00:01.3: SMBus Host Controller at 0xb100, revision 0
Mod-ips 554> device-mapper: ioctl: 4.14.0-ioctl (2008-04-23) initialised:
dm-devel@redhat.com
Mod-ips 555> cpuidle: using governor ladder
Mod-ips 556> usbcore: registered new interface driver usbhid
Mod-ips 557> usbhid: v2.6:USB HID core driver
Mod-ips 558> TCP cubic registered
Mod-ips 559> IPv6: Loaded, but is disabled by default. IPv6 may be enabled on individual
interf
Mod-ips 560> aces.
Mod-ips 561> NET: Registered protocol family 10
Mod-ips 562> NET: Registered protocol family 17
Mod-ips 563> NET: Registered protocol family 5
Mod-ips 564> rtc_cmos 00:01: setting system clock to 2012-01-17 14:06:34 UTC (1326809194)
Mod-ips 565> Freeing unused kernel memory: 1032k freed
Mod-ips 566> Write protecting the kernel read-only data: 4272k
Mod-ips 567> Loader init started...
Mod-ips 568> kjournald starting.  Commit interval 5 seconds
Mod-ips 569> EXT3-fs: mounted filesystem with ordered data mode.
Mod-ips 570> input: ImExPS/2 Generic Explorer Mouse as /class/input/input1
Mod-ips 571> 51216 blocks
Mod-ips 572> Checking rootrw fs: corrected filesystem
Mod-ips 573> kjournald starting.  Commit interval 5 seconds
Mod-ips 574> EXT3 FS on hda2, internal journal
Mod-ips 575> EXT3-fs: mounted filesystem with ordered data mode.
Mod-ips 576> mkdir: cannot create directory '/lib/modules': File exists
Mod-ips 577> init started: BusyBox v1.13.1 (2011-11-01 07:21:34 CDT)
Mod-ips 578> starting pid 678, tty '': '/etc/init.d/rc.init'
Mod-ips 579> Checking system fs: no errors
Mod-ips 580> kjournald starting.  Commit interval 5 seconds
Mod-ips 581> EXT3-fs: mounted filesystem with ordered data mode.
Mod-ips 582> /etc/init.d/rc.init: line 102: /proc/sys/vm/bdflush: No such file or
directory
Mod-ips 583> starting pid 728, tty '': '/etc/init.d/rcS'
Mod-ips 584> Initializing random number generator... done.
Mod-ips 585> Starting network... ifconfig lo 127.0.0.1 netmask 255.255.255.255 up
Mod-ips 586> starting inetd
Mod-ips 587> done
Mod-ips 588> Starting sshd:
Mod-ips 589> Starting nscd:
Mod-ips 590> Set Irq Affinity ... cpus:
Mod-ips 591> Checking kernel allocated memory: EXT3 FS on hda1, internal journal
Mod-ips 592> [  OK  ]
Mod-ips 593> Unloading REGEX-CP drivers ...
Mod-ips 594> Loading REGEX-CP drivers ...
```

```
Mod-ips 595> ACPI: PCI Interrupt Link [LNKD] enabled at IRQ 11
Mod-ips 596> cpp_user_kvm 0000:00:04.0: PCI INT A -> Link[LNKD] -> GSI 11 (level, high) ->
IRQ
Mod-ips 597> 11
Mod-ips 598> Detected cpp_user_kvm device with 33554432 bytes of shared memory
Mod-ips 599> Device 0: model=LCPX8640, cpc=T2005, cpe0=None, cpe1=None
Mod-ips 600> Load cidmodcap:
Mod-ips 601> Create node:
Mod-ips 602> ln: /etc/modprobe.conf: File exists
Mod-ips 603> Shutting down network... ifconfig lo down
Mod-ips 604> ifconfig lo down
Mod-ips 605> done
Mod-ips 606> Load ihm:
Mod-ips 607> Create node:
Mod-ips 608> Load kvm_ivshmem: IVSHMEM: writing 0x0 to 0xc86cf8
Mod-ips 609> IVSHMEM: IntrMask write(w) val = 0xffff
Mod-ips 610> Create node:
Mod-ips 611> Create node:
Mod-ips 612> Create node:
Mod-ips 613> Set Irq Affinity ... cpus: 6
Mod-ips 614> Starting network... ifconfig lo 127.0.0.1 netmask 255.255.255.255 up
Mod-ips 615> done
Mod-ips 616> Creating boot.info[  OK  ]
Mod-ips 617> Checking for system modifications since last boot[  OK  ]
Mod-ips 618> Checking model identification[  OK  ]
Mod-ips 619> Model: ASA-5555
Mod-ips 620> Model=ASA-5555
Mod-ips 621> Unable to set speed and duplex for user mode interfaces
Mod-ips 622> interface type 0x8086:0x100e at pci address 0:6.0(0) is currently named eth1
Mod-ips 623> Renaming eth1 --> ma0_0
Mod-ips 624> interface type 0x8086:0x100e at pci address 0:7.0(0) is currently named po0_0
Mod-ips 625> interface type 0x8086:0x100e at pci address 0:5.0(0) is currently named eth0
Mod-ips 626> Renaming eth0 --> sy0_0
Mod-ips 627> Initializing access list
Mod-ips 628> MGMT_INTFC_CIDS_NAME Management0/0
Mod-ips 629> MGMT_INTFC_OS_NAME ma0_0
Mod-ips 630> SYSTEM_PCI_IDS 0x0030,0x0028
Mod-ips 631> Load rebootkom:
Mod-ips 632> root: Starting SSM controlplane
Mod-ips 633> Starting CIDS:
Mod-ips 634> starting pid 1718, tty '/dev/ttyS0': '/sbin/getty -L ttyS0 9600 vt100'
```

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 18-23

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.
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-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:

	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-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.