Configuring the ASA 5585-X IPS SSP

This chapter contains procedures that are specific to configuring the ASA 5585-X IPS SSP. It contains the following sections:

ASA 5585-X IPS SSP Notes and Caveats

The following notes and caveats apply to configuring the ASA 5585-X IPS SSP:

- The ASA 5585-X IPS SSP is supported in ASA 8.2(4.4) and later as well as ASA 8.4(2) and later. It is not supported in ASA 8.3(*x*).
- All IPS platforms allow ten concurrent CLI sessions.
- Anomaly detection is disabled by default.
- The ASA 5585-X IPS SSP does not support CDP mode.
- The ASA 5585-X IPS SSP does not support the inline TCP session tracking mode.
- For the ASA 5585-X IPS SSP, normalization is performed by the adaptive security appliance and not the IPS.

- The ASA 5585-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 5585-X IPS SSP supports the String ICMP XL, String TCP XL, and String UDP XL engines. These engines provide optimized operation for these platforms.
- The ASA 5585-X IPS SSP has four types of ports (console, management, GigabitEthernet, and 10GE). The console and management ports (on the right front panel of the ASA 5585-X IPS SSP) are configured and controlled by IPS software. The GigabitEthernet and 10GE ports (on the left front panel of the ASA 5585-X IPS SSP) are configured and controlled by ASA software rather than IPS software. However, when you reset or shut down the ASA 5585-X IPS SSP, the GigabitEthernet and 10GE ports will also link down. You should reset or shut down the ASA 5585-X IPS SSP during scheduled maintenance windows to minimize the effect of the link down on these ports.

Configuration Sequence for the ASA 5585-X IPS SSP

Perform the following tasks to configure the ASA 5585-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 5585-X IPS SSP.
4. Run the **setup** command to initialize the ASA 5585-X IPS SSP.
5. Verify initialization for the ASA 5585-X IPS SSP.
6. Configure the adaptive security appliance to send IPS traffic to the ASA 5585-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 5585-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 5585-X IPS SSP when needed.

For More Information

- For the procedure for logging in to the ASA 5585-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 5585-X IPS SSP, page 3-17.
- For the procedure for verifying ASA 5585-X IPS SSP initialization, see Verifying Initialization for the ASA 5585-X IPS SSP, page 19-3.
- For the procedure for creating virtual sensors, see Creating Virtual Sensors for the ASA 5585-X IPS SSP, page 19-4.
- For the procedures for setting up the ASA 5585-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 5585-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 5585-X IPS SSP, see Installing the System Image for the ASA 5585-X IPS SSP Series, page 21-25.

Verifying Initialization for the ASA 5585-X IPS SSP

You can use the **show module** *slot* **details** command to verify that you have initialized the ASA 5585-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 5585-X IPS SSP.

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-10 with 8GE
Model:              ASA5585-SSP-IPS10
Hardware version:   1.0
Serial Number:      JAF1350ABSL
Firmware version:   2.0(1)3
Software version:   7.2(1)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
Mgmt TLS enabled    true
asa
```

Step 3 Confirm the information.

Creating Virtual Sensors for the ASA 5585-X IPS SSP

This section describes how to create virtual sensors on the ASA 5585-X IPS SSP, and contains the following topics:

The ASA 5585-X IPS SSP and Virtualization

The ASA 5585-X IPS SSP has two interfaces, the management interface (command and control) and the sensing interface. The command and control interface has an IP address and is used for configuring the ASA 5585-X IPS SSP. It is used by the ASA 5585-X IPS SSP to transmit security and status events to the IDM or IME. The ASA 5585-X IPS SSP command and control interface is named Management 0/0.

Caution The ASA 5585-X IPS SSP has four types of ports (console, management, GigabitEthernet, and 10GE). The console and management ports (on the right front panel of the ASA 5585-X IPS SSP) are configured and controlled by IPS software. The GigabitEthernet and 10GE ports (on the left front panel of the ASA 5585-X IPS SSP) are configured and controlled by ASA software rather than IPS software. However, when you reset or shut down the ASA 5585-X IPS SSP, the GigabitEthernet and 10GE ports will also link down. You should reset or shut down the ASA 5585-X IPS SSP during scheduled maintenance windows to minimize the effect of the link down on these ports.

The command and control interface is permanently enabled. It is permanently mapped to a specific physical interface. You cannot use the command and control interface as either a sensing or alternate TCP reset interface.

Sensing interfaces are used to analyze traffic for security violations. There is only one sensing interface on the ASA 5585-X IPS SSP. It is named PortChannel 0/0 and is a backplane interface. All backplane interfaces have fixed speed, duplex, and state settings. These settings are protected in the default configuration on all backplane interfaces. You configure the ASA 5585-X IPS SSP interface by security context on the adaptive security appliance. The sensing interface is permanently enabled. When you create multiple virtual sensors, you must assign the sensing 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.

The ASA 5585-X IPS SSP Virtual Sensor Configuration Sequence

Follow this sequence to create virtual sensors on the ASA 5585-X IPS SSP, and to assign them to adaptive security appliance contexts:

1. Configure up to four virtual sensors.
2. Assign the ASA 5585-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 5585-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 5585-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
   name: vs1
   -----------------------------------------------
      description: virtual sensor 1 default:
      signature-definition: sig1 default: sig0
      event-action-rules: rules1 default: rules0
      anomaly-detection
      -----------------------------------------------
         anomaly-detection-name: ad1 default: ad0
         operational-mode: learn default: detect
      -----------------------------------------------
      physical-interface (min: 0, max: 999999999, current: 2)
      -----------------------------------------------
         name: PortChannel0/0
         subinterface-number: 0 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      logical-interface (min: 0, max: 999999999, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
sensor(config-ana-vir)#
```

Step 10 Exit analysis engine mode.

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

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

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

For More Information

- For the procedures for creating and configuring anomaly detection policies, see Working With Anomaly Detection Policies, page 9-8.
- 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.
- For the procedure for enabling anomaly detection, see Enabling Anomaly Detection, page 9-8.

Assigning Virtual Sensors to Adaptive Security Appliance Contexts

After you create virtual sensors on the ASA 5585-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 5585-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 5585-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 5585-X IPS SSP and the Normalizer Engine

The majority of the features in the Normalizer engine are not used on the ASA 5585-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 5585-X IPS SSP and Bypass Mode

The ASA 5585-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 5585-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.

ASA 5585-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.

TCP Reset Differences Between IPS Appliances and the ASA 5585-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 5585-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 5585-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 5585-X IPS SSP

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

Use the following commands to reload, shut down, reset, recover the password, and recover the ASA 5585-X IPS SSP directly from the adaptive security appliance:

- **hw-module module** *slot_number* **reload—**This command reloads the software on the ASA 5585-X IPS SSP without doing a hardware reset. It is effective only when the module is in the Up state.
- **hw-module module** *slot_number* **shutdown—**This command shuts down the software on the ASA 5585-X IPS SSP. It is effective only when the module is in Up state.
- **hw-module module** *slot_number* **reset**—This command performs a hardware reset of the ASA 5585-X IPS SSP. It is applicable when the module is in the Up/Down/Unresponsive/Recover states.
- **hw-module module** *slot_number* **password-reset—**This command restores the cisco CLI account password on the ASA 5585-X IPS SSP to the default **cisco**.
- **hw-module module** *slot_number* **recover** [**boot | stop | configure**]—The **recover** command displays a set of interactive options for setting or changing the recovery parameters. To change the parameter or keep the existing setting, press **Enter**.
  - **hw-module module** *slot_number* **recover boot**—This command initiates recovery of the ASA 5585-X IPS SSP. It is applicable only when the module is in the Up state.
  - **hw-module module** *slot_number* **recover stop**—This command stops recovery of the ASA 5585-X IPS SSP. It is applicable only when the module is in the Recover state.

Caution If the ASA 5585-X IPS SSP recovery needs to be stopped, you must issue the **hw-module module 1 recover stop** command within 30 to 45 seconds after starting the recovery. Waiting any longer can lead to unexpected consequences. For example, the module may come up in the Unresponsive state.

- **hw-module module 1 recover configure**—Use this command to configure parameters for the ASA 5585-X IPS SSP recovery. The essential parameters are the IP address and recovery image TFTP URL location.

  Example

```
ips-ssp# hardware-module module 1 recover configure
Image URL [tftp://10.89.146.1/IPS-SSP_10-K9-sys-1.1-a-7.2-1-E4.img]:
Port IP Address [10.89.149.226]:
VLAN ID [0]:
Gateway IP Address [10.89.149.254]:
```

For More Information

For the procedure for recovering the ASA 5585-X IPS SSP system image, see Installing the System Image for the ASA 5585-X IPS SSP Series, page 21-25.

Health and Status Information

To see the general health of the ASA 5585-X IPS SSP, use the **show module 1 details** command.

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(1)3
Software version:   7.2(1)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
Mgmt TLS enabled    true
asa
```

The output shows that the ASA 5585-X IPS SSP is up. If the status reads `Down`, you can reset it using the **hw-module module 1 reset** command.

```
asa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm]
Reset issued for module in slot 1
asa# show module 1 details
Getting details from the Service Module, please wait...
```

```
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.2(1)E4
Data plane Status:  Not Applicable
Status:             Shutting Down
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.2(1)E4
Data plane Status:  Not Applicable
Status:             Down
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.2(1)E4
Data plane Status:  Not Applicable
Status:             Init
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Reload
App. Status Desc:   Starting up
App. version:       7.2(1)E4
Data plane Status:  Down
Status:             Up
Mgmt IP addr:       192.0.2.3
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# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.3
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#
```

If you have problems with reimaging the ASA 5585-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 **hw-module module 1 recover** command again to reimage the module.

```
ips-ssp# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.10.10.10//IPS-SSP_20-K9-sys-1.1-a-7.2-1-E4.img
Port IP Address [0.0.0.0]: 10.10.10.11
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.10.10.254

asa(config)# debug module-boot
debug module-boot enabled at level 1
asa(config)# hw-module module 1 recover boot
The module in slot 1 will be recovered. This may erase all configuration and all data on
that device and attempt to download a new image for it.
Recover module in slot 1? [confirm]
Recover issued for module in slot 1
asa(config)# Slot-1 140> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10
PST 2010
Slot-1 141> Platform ASA5585-SSP-IPS20
Slot-1 142> GigabitEthernet0/0
Slot-1 143> Link is UP
Slot-1 144> MAC Address: 000b.fcf8.0176
Slot-1 145> ROMMON Variable Settings:
Slot-1 146>   ADDRESS=192.0.2.3
Slot-1 147>   SERVER=192.0.2.15
Slot-1 148>   GATEWAY=192.0.2.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSP-K9-sys-1.1-a-7.2-1.img
Slot-1 152>   CONFIG=
Slot-1 153>   LINKTIMEOUT=20
Slot-1 154>   PKTTIMEOUT=4
Slot-1 155>   RETRY=20
Slot-1 156> tftp IPS-SSP_10-K9-sys-1.1-a-7.2-1.img@192.0.2.15 via 192.0.2.254
Slot-1 157> TFTP failure: Packet verify failed after 20 retries
```

```
Slot-1 158> Rebooting due to Autoboot error ...
Slot-1 159> Rebooting....
Slot-1 160> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10 PST 2010
Slot-1 161> Platform ASA5585-SSP-IPS20
Slot-1 162> GigabitEthernet0/0
Slot-1 163> Link is UP
Slot-1 164> MAC Address: 000b.fcf8.0176
Slot-1 165> ROMMON Variable Settings:
Slot-1 166>   ADDRESS=192.0.2.3
Slot-1 167>   SERVER=192.0.2.15
Slot-1 168>   GATEWAY=192.0.2.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSP_10-K9-sys-1.1-a-7.2-1.img
Slot-1 172>   CONFIG=
Slot-1 173>   LINKTIMEOUT=20
Slot-1 174>   PKTTIMEOUT=4
Slot-1 175>   RETRY=20
Slot-1 176> tftp IPS-SSP_10-K9-sys-1.1-a-7.2-1.img@192.0.2.15 via 192.0.2.254
```

Traffic Flow Stopped on IPS Switchports

Problem Traffic on any port located on the ASA 5585-X IPS SSP (1/x) no longer passes through the adaptive security appliance when the ASA 5585-X IPS SSP is reset or shut down. This affects all traffic through these ports regardless of whether or not the traffic would have been monitored by the IPS. The link on the ports will link down when the ASA 5585-X IPS SSP is reset or shut down.

Possible Cause Using the ports located on the ASA 5585-X IPS SSP (1/x), and resetting or shutting it down via any mechanism.

Solution Use the ports on the adaptive security appliance (0/x) instead because those ports do not lose their link when the ASA 5585-X IPS SSP is reset or shut down.

Failover Scenarios

The following failover scenarios apply to the ASA 5585-X in the event of configuration changes, signature/signature engine updates, service packs, and SensorApp crashes on the ASA 5585-X IPS SSP.

Single ASA 5585-X in Fail-Open Mode

- If the ASA is configured in fail-open mode for the ASA 5585-X IPS SSP, and the ASA 5585-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 5585-X IPS SSP, and the ASA 5585-X IPS SSP experiences a SensorApp crash or a service pack upgrade, traffic is passed through the ASA without being inspected.

Single ASA 5585-X in Fail-Close Mode

- If the ASA is configured in fail-close mode for the ASA 5585-X IPS SSP, and the ASA 5585-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 5585-X IPS SSP, and the ASA 5585-X IPS SSP experiences a SensorApp crash or a service pack upgrade, traffic is stopped from passing through the ASA.

Two ASA 5585-Xs in Fail-Open Mode

- If the ASAs are configured in fail-open mode and if the ASA 5585-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 5585-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 5585-X IPS SSP that was previously the standby ASA 5585-X IPS SSP.

Two ASA 5585-Xs in Fail-Close Mode

- If the ASAs are configured in fail-close mode, and if the ASA 5585-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 5585-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 5585-X IPS SSP that was previously the standby for the ASA 5585-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
```