CHAPTER 23

Managing the AIP SSM and CSC SSM

This chapter describes how to configure the adaptive security appliance to support an AIP SSM or a CSC SSM that is installed in the adaptive security appliance.

See Chapter 6, "Configuring Ethernet Settings, Redundant Interfaces, and Subinterfaces" for information about the 4GE SSM for the ASA 5500 series adaptive security appliance.

Note The Cisco PIX 500 series security appliances do not support SSMs. The ASA 5510, ASA 5520, and ASA 5540 series adaptive security appliances support SSMs.

This chapter includes the following sections:

Managing the AIP SSM

This section includes the following topics:

AIP SSM Overview

You can install the AIP SSM into an ASA 5500 series adaptive security appliance. The AIP SSM runs advanced IPS software that provides proactive, full-featured intrusion prevention services to stop malicious traffic, including worms and network viruses, before they can affect your network. This section includes the following topics:

How the AIP SSM Works with the Adaptive Security Appliance

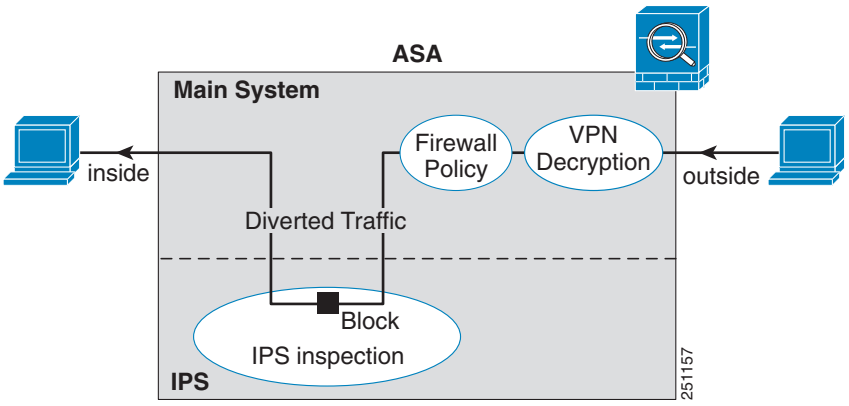
The AIP SSM runs a separate application from the adaptive security appliance. It is, however, integrated into the adaptive security appliance traffic flow. The AIP SSM does not contain any external interfaces itself, other than a management interface. When you identify traffic for IPS inspection on the adaptive security appliance, traffic flows through the adaptive security appliance and the AIP SSM in the following way:

1. Traffic enters the adaptive security appliance.
2. Incoming VPN traffic is decrypted.
3. Firewall policies are applied.
4. Traffic is sent to the AIP SSM over the backplane.

   See the "Operating Modes" section on page 23-3 for information about only sending a copy of the traffic to the AIP SSM.
5. The AIP SSM applies its security policy to the traffic, and takes appropriate actions.
6. Valid traffic is sent back to the adaptive security appliance over the backplane; the AIP SSM might block some traffic according to its security policy, and that traffic is not passed on.
7. Outgoing VPN traffic is encrypted.
8. Traffic exits the adaptive security appliance.

Figure 23-1 shows the traffic flow when running the AIP SSM in inline mode. In this example, the AIP SSM automatically blocks traffic that it identified as an attack. All other traffic is forwarded through the adaptive security appliance.

Figure 23-1 AIP SSM Traffic Flow in the Adaptive Security Appliance: Inline Mode

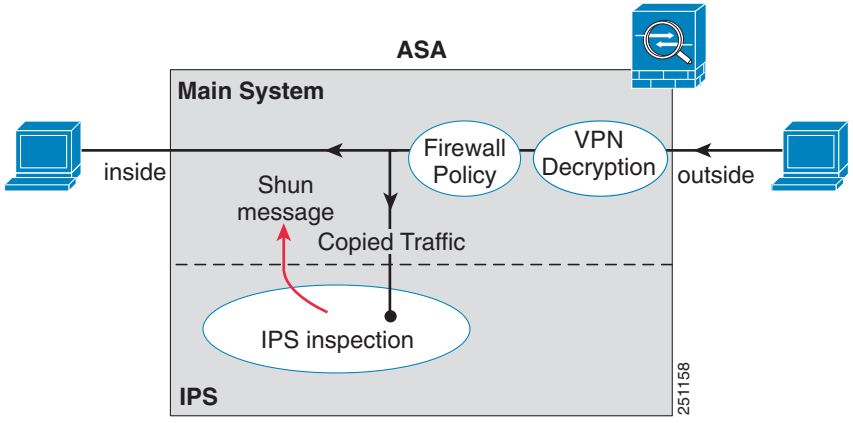


Operating Modes

You can send traffic to the AIP SSM using one of the following modes:

- Inline mode—This mode places the AIP SSM directly in the traffic flow (see Figure 23-1). No traffic that you identified for IPS inspection can continue through the adaptive security appliance without first passing through, and being inspected by, the AIP SSM. This mode is the most secure because every packet that you identify for inspection is analyzed before being allowed through. Also, the AIP SSM can implement a blocking policy on a packet-by-packet basis. This mode, however, can affect throughput.
- Promiscuous mode—This mode sends a duplicate stream of traffic to the AIP SSM. This mode is less secure, but has little impact on traffic throughput. Unlike the inline mode, in promiscuous mode the AIP SSM can only block traffic by instructing the adaptive security appliance to shun the traffic or by resetting a connection on the adaptive security appliance. Also, while the AIP SSM is analyzing the traffic, a small amount of traffic might pass through the adaptive security appliance before the AIP SSM can shun it. Figure 23-2 shows the AIP SSM in promiscuous mode. In this example, the AIP SSM sends a shun message to the security appliance for traffic it identified as a threat.

Figure 23-2 AIP SSM Traffic Flow in the Adaptive Security Appliance: Promiscuous Mode



Using Virtual Sensors

The AIP SSM running IPS software Version 6.0 and above can run multiple virtual sensors, which means you can configure multiple security policies on the AIP SSM. You can assign each context or single mode security appliance to one or more virtual sensors, or you can assign multiple security contexts to the same virtual sensor. See the IPS documentation for more information about virtual sensors, including the maximum number of sensors supported.

Figure 23-3 shows one security context paired with one virtual sensor (in inline mode), while two security contexts share the same virtual sensor.

Figure 23-3 Security Contexts and Virtual Sensors

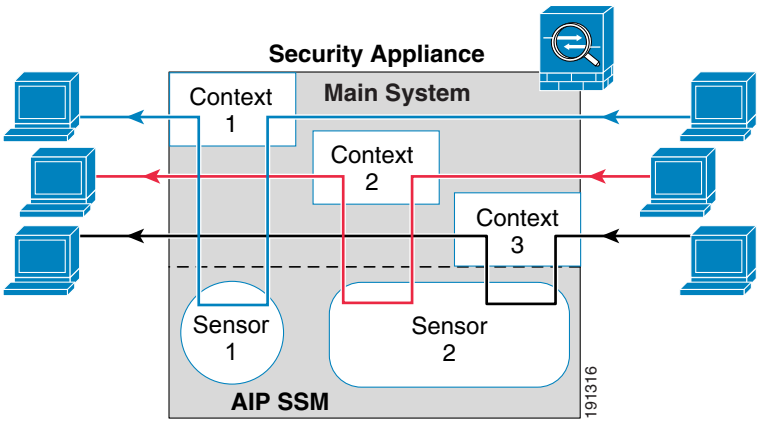
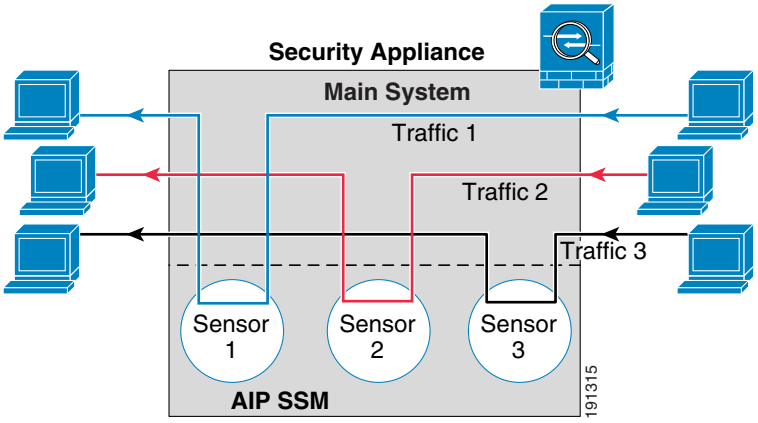


Figure 23-4 shows a single mode security appliance paired with multiple virtual sensors (in inline mode); each defined traffic flow goes to a different sensor.

Figure 23-4 Single Mode Security Appliance with Multiple Virtual Sensors



AIP SSM Procedure Overview

Configuring the AIP SSM is a process that includes configuration of the AIP SSM and then configuration of the ASA 5500 series adaptive security appliance:

1. Session to the AIP SSM from the security appliance. See the "Sessioning to the AIP SSM" section on page 23-5.
2. On the AIP SSM, configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. Configure the inspection and protection policy for each virtual sensor if you want to run the AIP SSM in multiple sensor mode. See the "Configuring the Security Policy on the AIP SSM" section on page 23-6.
3. On the ASA 5500 series adaptive security appliance in multiple context mode, specify which IPS virtual sensors are available for each context (if you configured virtual sensors). See the "Assigning Virtual Sensors to Security Contexts" section on page 23-6.
4. On the ASA 5500 series adaptive security appliance, identify traffic to divert to the AIP SSM. See the "Diverting Traffic to the AIP SSM" section on page 23-8.

Sessioning to the AIP SSM

To begin configuring the AIP SSM, session to the AIP SSM from the adaptive security appliance. (You can alternatively connect directly to the AIP SSM management interface using SSH or Telnet.)

To session to the AIP SSM from the adaptive security appliance, perform the following steps:

Step 1 To session from the ASA 5500 series adaptive security appliance to the AIP SSM, enter the following command:

```
hostname# session 1

Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 2 Enter the username and password. The default username and password is “cisco.”

Note The first time you log in to the AIP SSM, you are prompted to change the default password. Passwords must be at least eight characters long and not a word in the dictionary.

```
login: cisco
Password:
Last login: Fri Sep 2 06:21:20 from xxx.xxx.xxx.xxx
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
AIP SSM#
```

Note If you see the preceding license notice (which displays only in some versions of software), you can ignore the message until you need to upgrade the signature files on the AIP SSM. The AIP SSM continues to operate at the current signature level until a valid license key is installed. You can install the license key at a later time. The license key does not affect the current functionality of the AIP SSM.

Configuring the Security Policy on the AIP SSM

On the AIP SSM, to configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected, perform the following steps. To session from the security appliance to the AIP SSM, see the "Sessioning to the AIP SSM" section on page 23-5.

Step 1 To run the setup utility for initial configuration of the AIP SSM, enter the following command:

```
sensor# setup
```

Step 2 Configure the IPS security policy. If you configure virtual sensors in IPS Version 6.0 or above, you identify one of the sensors as the default. If the ASA 5500 series adaptive security appliance does not specify a virtual sensor name in its configuration, the default sensor is used.

Because the IPS software that runs on the AIP SSM is beyond the scope of this document, detailed configuration information is available at the following URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

Step 3 When you are done configuring the AIP SSM, exit the IPS software by entering the following command:

```
sensor# exit
```

If you sessioned to the AIP SSM from the security appliance, you return to the security appliance prompt.

Assigning Virtual Sensors to Security Contexts

If the security appliance is in multiple context mode, then you can assign one or more IPS virtual sensors to each context. Then, when you configure the context to send traffic to the AIP SSM, 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 AIP SSM is used. You can assign the same sensor to multiple contexts.

Note You do not need to be in multiple context mode to use virtual sensors; you can be in single mode and use different sensors for different traffic flows.

To assign one or more sensors to a security context, perform the following steps:

Step 1 To enter context configuration mode, enter the following command in the system execution space:

```
hostname(config)# context name
hostname(config-ctx)#
```

For more information about configuring contexts, see the "Configuring a Security Context" section on page 7-7.

Step 2 To assign a virtual sensor to the context, enter the following command:

```
hostname(config-ctx)# allocate-ips sensor_name [mapped_name] [default]
```

Enter this command for each sensor you want to assign to the context.

The *sensor _name* argument is the sensor name configured on the AIP SSM. To view the sensors that are configured on the AIP SSM, enter **allocate-ips ?**. All available sensors are listed. You can also enter the **show ips** command. In the system execution space, the **show ips** command lists all available sensors; if you enter it in the context, it shows the sensors you already assigned to the context. If you specify a sensor name that does not yet exist on the AIP SSM, you get an error, but the **allocate-ips** command is entered as is. Until you create a sensor of that name on the AIP SSM, the context assumes the sensor is down.

Use the *mapped_name* argument 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.

The **default** keyword 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 AIP SSM.

Step 3 Repeat Step 1 and Step 2 for each context.

Step 4 To configure the context IPS policy, change to the context execution space using the following command:

```
hostname(config-ctx)# changeto context context_name
```

where the *context_name* argument is the name of the context you want to configure. Change to each context to configure the IPS security policy as described in "Diverting Traffic to the AIP SSM" section on page 23-8.

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 AIP SSM is used.

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1
hostname(config-ctx)# allocate-ips sensor3 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver

hostname(config-ctx)# changeto context A
...
```

Diverting Traffic to the AIP SSM

To identify traffic to divert from the adaptive security appliance to the AIP SSM, perform the following steps. In multiple context mode, perform these steps in each context execution space.

Step 1 To identify the traffic that you want to be inspected by the AIP SSM, add one or more class maps using the **class-map** command according to the "Creating a Layer 3/4 Class Map for Through Traffic" section on page 16-5.

For example, you can match all traffic using the following commands:

```
hostname(config)# class-map IPS
hostname(config-cmap)# match any
```

To match specific traffic, you can match an access list:

```
hostname(config)# access list IPS extended permit ip any 10.1.1.1 255.255.255.255
hostname(config)# class-map IPS
hostname(config-cmap)# match access-list IPS
```

Step 2 To add or edit a policy map that sets the action to divert traffic to the AIP SSM, enter the following commands:

```
hostname(config)# policy-map name
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

where the *class_map_name* is the class map from Step 1.

For example:

```
hostname(config)# policy-map IPS
hostname(config-pmap)# class IPS
```

Step 3 To divert the traffic to the AIP SSM, enter the following command:

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close | fail-open} [sensor
{sensor_name | mapped_name}]
```

where the **inline** and **promiscuous** keywords control the operating mode of the AIP SSM. See the "Operating Modes" section on page 23-3 for more details.

The **fail-close** keyword sets the adaptive security appliance to block all traffic if the AIP SSM is unavailable.

The **fail-open** keyword sets the adaptive security appliance to allow all traffic through, uninspected, if the AIP SSM is unavailable.

If you use virtual sensors on the AIP SSM, you can specify a sensor name using the **sensor** *sensor_name* argument. To see available sensor names, enter the **ips ... sensor ?** command. Available sensors are listed. You can also use the **show ips** command. If you use multiple context mode on the security appliance, you can only specify sensors that you assigned to the context (see the "Assigning Virtual Sensors to Security Contexts" section on page 23-6). Use the *mapped_name* if configured in the context. If you do not specify a sensor name, then the traffic uses the default sensor. In multiple context mode, you can specify a default sensor for the context. In single mode or if you do not specify a default sensor in multiple mode, the traffic uses the default sensor that is set on the AIP SSM. If you enter a name that does not yet exist on the AIP SSM, you get an error, and the command is rejected.

Step 4 (Optional) To divert another class of traffic to the AIP SSM, and set the IPS policy, enter the following commands:

```
hostname(config-pmap-c)# class class_map_name2
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close | fail-open} [sensor
sensor_name]
```

where the *class_map_name2* argument is the name of a separate class map on which you want to perform IPS inspection. See Step 3 for information about the command options. See the "Information About Layer 3/4 Policy Maps" section on page 16-17 for detailed information about how the order of classes matters within a policy map. Traffic cannot match more than one class map for the same action type; so if you want network A to go to sensorA, but want all other traffic to go to sensorB, then you need to enter the **class** command for network A before you enter the **class** command for all traffic; otherwise all traffic (including network A) will match the first **class** command, and will be sent to sensorB.

Step 5 To activate the policy map on one or more interfaces, enter the following command:

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface interface_ID]
hostname
```

where *policy_map_name* is the policy map you configured in Step 2. To apply the policy map to traffic on all the interfaces, use the **global** keyword. To apply the policy map to traffic on a specific interface, use the **interface** *interface_ID* option, where *interface_ID* is the name assigned to the interface with the **nameif** command.

Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

The following example diverts all IP traffic to the AIP SSM in promiscuous mode, and blocks all IP traffic if the AIP SSM card fails for any reason:

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

The following example diverts all IP traffic destined for the 10.1.1.0 network and the 10.2.1.0 network to the AIP SSM in inline mode, and allows all traffic through if the AIP SSM card fails for any reason. For the my-ips-class traffic, sensor1 is used; for the my-ips-class2 traffic, sensor2 is used.

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
hostname(config)# class-map my-ips-class2
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface outside
```

Managing the CSC SSM

This section includes the following topics:

About the CSC SSM

The ASA 5500 series adaptive security appliance supports the CSC SSM, which runs Content Security and Control software. The CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic by scanning the FTP, HTTP, POP3, and SMTP packets that you configure the adaptive security appliance to send to it.

Figure 23-5 illustrates the flow of traffic through an adaptive security appliance that has the following:

- A CSC SSM installed and configured.
- A service policy that determines what traffic is diverted to the CSC SSM for scanning.

In this example, the client could be a network user who is accessing a website, downloading files from an FTP server, or retrieving mail from a POP3 server. SMTP scans differ in that you should configure the adaptive security appliance to scan traffic sent from the outside to SMTP servers protected by the adaptive security appliance.

Note The CSC SSM can scan FTP file transfers only when FTP inspection is enabled on the adaptive security appliance. By default, FTP inspection is enabled.

Figure 23-5 Flow of Scanned Traffic with CSC SSM

You use ASDM for system setup and monitoring of the CSC SSM. For advanced configuration of content security policies in the CSC SSM software, you access the web-based GUI for the CSC SSM by clicking links within ASDM. For instructions on use of the CSC SSM GUI, see the *Trend Micro InterScan for Cisco CSC SSM Administrator Guide*.

Note ASDM and the CSC SSM maintain separate passwords. You can configure their passwords to be identical; however, changing one of these two passwords does not affect the other password.

The connection between the host running ASDM and the adaptive security appliance is made through a management port on the adaptive security appliance. The connection to the CSC SSM GUI is made through the SSM management port. Because these two connections are required to manage the CSC SSM, any host running ASDM must be able to reach the IP address of both the adaptive security appliance management port and the SSM management port.

Figure 23-6 shows an adaptive security appliance with a CSC SSM that is connected to a dedicated management network. While use of a dedicated management network is not required, we recommend it. Of particular interest are the following:

- An HTTP proxy server is connected to the inside network and to the management network. This HTTP proxy server enables the CSC SSM to contact the Trend Micro update server.
- The management port of the adaptive security appliance is connected to the management network. To permit management of the adaptive security appliance and the CSC SSM, hosts running ASDM must be connected to the management network.
- The management network includes an SMTP server for e-mail notifications for the CSC SSM and a syslog server to which the CSC SSM can send system log messages.

Figure 23-6 CSC SSM Deployment with a Management Network

The CSC SSM cannot support Stateful Failover because the CSC SSM does not maintain connection information, and therefore cannot provide the failover unit with the required information for Stateful Failover. The connections that a CSC SSM is scanning are dropped when the security appliance in which the CSC SSM is installed fails. When the standby adaptive security appliance becomes active, it will forward the scanned traffic to the CSC SSM and the connections will be reset.

Getting Started with the CSC SSM

Before you receive the security benefits provided by a CSC SSM, you must perform several steps beyond hardware installation of the SSM. This procedure provides an overview of those steps.

To configure the adaptive security appliance and the CSC SSM, follow these steps:

Step 1 If the CSC SSM did not come pre-installed in a Cisco ASA 5500 series adaptive security appliance, install it and connect a network cable to the management port of the SSM. For assistance with installation and connecting the SSM, see the *Cisco ASA 5500 Series Hardware Installation Guide*.

The management port of the CSC SSM must be connected to your network to allow management of and automatic updates to the CSC SSM software. Additionally, the CSC SSM uses the management port for e-mail notifications and system log messaging.

Step 2 With the CSC SSM, you should have received a Product Authorization Key (PAK). Use the PAK to register the CSC SSM at the following URL.

`http://www.cisco.com/go/license`

After you register, you will receive activation keys by e-mail. The activation keys are required before you can complete Step 6

Step 3 Gather the following information for use in Step 6.

- Activation keys, received after completing Step 2.
- The CSC SSM management port IP address, netmask, and gateway IP address.

Note The CSC SSM management port IP address must be accessible by the hosts used to run ASDM. The IP addresses for the CSC SSM management port and the adaptive security appliance management interface can be in different subnets.

- DNS server IP address.
- HTTP proxy server IP address (needed only if your security policies require the use of a proxy server for HTTP access to the Internet).
- Domain name and hostname for the CSC SSM.
- An e-mail address and an SMTP server IP address and port number for e-mail notifications.
- IP addresses of hosts or networks allowed to manage the CSC SSM.
- Password for the CSC SSM.

Step 4 In a web browser, access ASDM for the adaptive security appliance in which the CSC SSM is installed.

Note If you are accessing ASDM for the first time, see the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* for assistance with the Startup Wizard.

For more information about enabling ASDM access, see the "Allowing HTTPS Access for ASDM" section on page 42-4.

Step 5 Verify time settings on the adaptive security appliance. Time setting accuracy is important for logging of security events and for automatic updates of CSC SSM software.

- If you manually control time settings, verify the clock settings, including time zone. Choose **Configuration > Properties > Device Administration > Clock**.

- If you are using NTP, verify the NTP configuration. Choose **Configuration > Properties > Device Administration > NTP**.

Step 6 To access the ASDM GUI in a supported web browser and on the Home page, click the **Content Security** tab. In ASDM, run the CSC Setup Wizard. To access the CSC Setup Wizard, choose **Configuration > Trend Micro Content Security > CSC Setup > Wizard Setup > Launch Setup Wizard**. The CSC Setup Wizard appears. For assistance with the CSC Setup Wizard, click the **Help** button.

Note If you are accessing ASDM for the first time, see the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* for assistance with the Startup Wizard.

Step 7 On the ASA 5500 series adaptive security appliance, identify traffic to divert to the CSC SSM (see the "Diverting Traffic to the CSC SSM" section on page 23-16).

Step 8 (Optional) Review the default content security policies in the CSC SSM GUI. The default content security policies are suitable for most implementations. Before you modify them or enter advanced configuration settings, review the *Trend Micro InterScan for Cisco CSC SSM Administrator Guide*.

You review the content security policies by viewing the enabled features in the CSC SSM GUI. The availability of features depends on the license level you have purchased. By default, all features included in the license you have purchased are enabled.

With a Base License, the features enabled by default are SMTP virus scanning, POP3 virus scanning and content filtering, webmail virus scanning, HTTP file blocking, FTP virus scanning and file blocking, logging, and automatic updates.

With a Plus License, the additional features enabled by default are SMTP anti-spam, SMTP content filtering, POP3 anti-spam, URL blocking, and URL filtering.

To access the CSC SSM GUI, in ASDM choose **Configuration > Trend Micro Content Security**, and then select one of the following: **Web**, **Mail**, **File Transfer**, or **Updates**. The links on these panes, beginning with the word "Configure," open the CSC SSM GUI.

Determining What Traffic to Scan

The CSC SSM can scan FTP, HTTP, POP3, and SMTP traffic only when the destination port of the packet requesting the connection is the well-known port for the specified protocol. The CSC SSM can scan only the following connections:

- FTP connections opened to TCP port 21.
- HTTP connections opened to TCP port 80.
- POP3 connections opened to TCP port 110.
- SMTP connections opened to TCP port 25.

You can choose to scan traffic for all of these protocols or any combination of them. For example, if you do not allow network users to receive POP3 e-mail, do not configure the adaptive security appliance to divert POP3 traffic to the CSC SSM. Instead, block this traffic.

To maximize performance of the adaptive security appliance and the CSC SSM, divert to the CSC SSM only the traffic that you want the CSC SSM to scan. Needlessly diverting traffic that you do not want to scan, such as traffic between a trusted source and destination, can adversely affect network performance.

To enable traffic scanning with the CSC SSM, use the **csc** command, which must be part of a service policy. Service policies can be applied globally or to specific interfaces; therefore, you can enable the **csc** command globally or for specific interfaces.

Adding the **csc** command to your global policy ensures that all unencrypted connections through the adaptive security appliance are scanned by the CSC SSM; however, this setting may mean that traffic from trusted sources is needlessly scanned.

If you enable the **csc** command in interface-specific service policies, it is bi-directional. Bi-directionality means that when the adaptive security appliance opens a new connection, if the **csc** command is active on either the inbound or the outbound interface of the connection and the class map for the policy identifies traffic for scanning, the adaptive security appliance diverts this traffic to the CSC SSM.

However, bi-directionality also means that if you divert any of the supported traffic types that cross a given interface to the CSC SSM, it is probably performing unnecessary scans on traffic from your trusted inside networks. For example, URLs and files requested from web servers on a DMZ network are unlikely to pose content security risks to hosts on an inside network, and you probably do not want the adaptive security appliance to divert this traffic to the CSC SSM.

Therefore, we recommend using access lists to further limit the traffic selected by the class maps of CSC SSM service policies. Specifically, use access lists that match the following:

- HTTP connections to outside networks.
- FTP connections from clients inside the adaptive security appliance to servers outside the adaptive security appliance.
- POP3 connections from clients inside the security appliance to servers outside the adaptive security appliance.
- Incoming SMTP connections destined to inside mail servers.

In Figure 23-7, the adaptive security appliance should be configured to divert traffic to CSC SSM requests from clients on the inside network for HTTP, FTP, and POP3 connections to the outside network and incoming SMTP connections from outside hosts to the mail server on the DMZ network. HTTP requests from the inside network to the web server on the DMZ network should not be scanned.

Figure 23-7 Common Network Configuration for CSC SSM Scanning

To identify the traffic that you want to scan, you can configure the adaptive security appliance in different ways. One approach is to define two service policies, one on the inside interface and the other on the outside interface, each with an access list that matches traffic to be scanned. The following access list can be used on the policy applied to the inside interface:

```
access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110
```

As previously mentioned, policies applying the **csc** command to a specific interface are effective on both ingress and egress traffic. However, by specifying 192.168.10.0 as the source network in the csc_out access list, the policy applied to the inside interface matches only connections initiated by the hosts on the inside network. Notice also that the second ACE of the access list contains the **deny** keyword. This ACE does not mean the adaptive security appliance blocks traffic sent from the 192.168.10.0 network to TCP port 80 on the 192.168.20.0 network. Instead, the ACE exempts the traffic from being matched by the policy map and thus prevents the adaptive security appliance from sending the traffic to the CSC SSM.

You can use **deny** keywords in an access list to exempt connections with trusted external hosts from being scanned. For better performance, if the CSC SSM traffic passes through the security appliance to reach the Internet, we recommend that you exempt the traffic generated by the CSC SSM itself from being scanned.

For example, to reduce the load on the CSC SSM, you might want to exempt HTTP traffic to a well-known, trusted site. If the web server at this site has the IP address 209.165.201.7, you could add the following ACE to the csc_out access list to exclude HTTP connections between the trusted external web server and inside hosts from being scanned by the CSC SSM:

```
access-list csc_out deny tcp 192.168.10.0 255.255.255.0 209.165.201.7 255.255.255.255 eq 80
```

The second policy in this example, applied to the outside interface, could use the following access list:

```
access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
```

This access list matches inbound SMTP connections from any external host to any host on the DMZ network. The policy applied to the outside interface would therefore ensure that incoming SMTP e-mail would be diverted to the CSC SSM for scanning. However, the policy would not match SMTP connections from hosts on the inside network to the mail server on the DMZ network, because those connections never use the outside interface.

If the web server on the DMZ network receives files uploaded by HTTP from external hosts, you could add the following ACE to the csc_in access list to use the CSC SSM to protect the web server from infected files:

```
access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80
```

For a service policy configuration using the access lists in this section, see Example 23-1.

Limiting Connections Through the CSC SSM

The adaptive security appliance can prevent the CSC SSM and the destinations of connections it scans from accepting or even receiving requests for more connections than desired. It can do so for embryonic connections or fully established connections. Also, you can specify limits for all clients included in a class-map and per-client limits. The **set connection** command lets you configure limits for embryonic connections or fully established connections.

Also, you can specify limits for all clients included in a class-map and per-client limits. The **per-client-embryonic-max** and **per-client-max** parameters limit the maximum number of connections that individual clients can open. If a client uses more network resources simultaneously than is desired, you can use these parameters to limit the number of connections that the adaptive security appliance allows for each client.

DoS attacks seek to disrupt networks by overwhelming the capacity of key hosts with connections or requests for connections. You can use the **set connection** command to thwart DoS attacks. After you configure a per-client maximum that can be supported by hosts likely to be attacked, malicious clients will be unable to overwhelm hosts on protected networks.

For use of the **set connection** command to protect the CSC SSM and the destinations of connections it scans, see the "Diverting Traffic to the CSC SSM" section on page 23-16.

Diverting Traffic to the CSC SSM

You use Modular Policy Framework commands to configure the adaptive security appliance to divert traffic to the CSC SSM. Before configuring the adaptive security appliance to divert traffic to the CSC SSM, review Chapter 16, "Using Modular Policy Framework," which introduces Modular Policy Framework concepts and common commands.

To identify traffic to divert from the adaptive security appliance to the CSC SSM, perform the following steps:

Step 1 Create an access list that matches the traffic you want scanned by the CSC SSM with the **access-list extended** command. Create as many ACEs as are needed to match all the traffic. For example, to specify FTP, HTTP, POP3, and SMTP traffic, you need four ACEs. For guidance on identifying the traffic you want to scan, see the "Determining What Traffic to Scan" section on page 23-13.

Step 2 Create a class map to identify the traffic that should be diverted to the CSC SSM with the **class-map** command:

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

where *class_map_name* is the name of the traffic class. When you enter the **class-map** command, the CLI enters class map configuration mode.

Step 3 With the access list you created in Step 1, use a **match access-list** command to identify the traffic to be scanned:

```
hostname(config-cmap)# match access-list acl-name
```

where *acl-name* is the name of the access list.

Step 4 Create a policy map or modify an existing policy map that you want to use to send traffic to the CSC SSM with the **policy-map** command:

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

where *policy_map_name* is the name of the policy map. The CLI enters the policy map configuration mode and the prompt changes accordingly.

Step 5 Specify the class map, created in Step 2, that identifies the traffic to be scanned. Use the **class** command to do so, as follows.

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

where *class_map_name* is the name of the class map you created in Step 2. The CLI enters the policy map class configuration mode and the prompt changes accordingly.

Step 6 If you want to enforce a per-client limit for simultaneous connections that the adaptive security appliance diverts to the CSC SSM, use the **set connection** command, as follows:

```
hostname(config-pmap-c)# set connection per-client-max n
```

where *n* is the maximum simultaneous connections the adaptive security appliance will allow per client. This command prevents a single client from abusing the services of the CSC SSM or any server protected by the SSM, including prevention of attempts at DoS attacks on HTTP, FTP, POP3, or SMTP servers that the CSC SSM protects.

Step 7 Assign the traffic identified by the class map as traffic to be sent to the CSC SSM with the **csc** command:

```
hostname(config-pmap-c)# csc {fail-close | fail-open}
```

The **fail-close** and **fail-open** keywords control how the adaptive security appliance handles traffic when the CSC SSM is unavailable. For more information about the operating modes and failure behavior, see the "About the CSC SSM" section on page 23-10.

Step 8 Apply the policy map globally or to a specific interface with the **service-policy** command:

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface interface_ID]
```

where *policy_map_name* is the policy map you configured in Step 4. To apply the policy map to traffic on all the interfaces, use the **global** keyword.To apply the policy map to traffic on a specific interface, use the **interface** *interface_ID* option, where *interface_ID* is the name assigned to the interface with the **nameif** command.

Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

The adaptive security appliance begins diverting traffic to the CSC SSM as specified.

Example 23-1 is based on the network shown in Figure 23-7 and shows the creation of two service policies:

- The first policy, csc_out_policy, is applied to the inside interface and uses the csc_out access list to ensure that all outbound requests for FTP and POP3 are scanned. The csc_out access list also ensures that HTTP connections from inside to networks on the outside interface are scanned, but it includes a deny ACE to exclude HTTP connections from inside to servers on the DMZ network.
- The second policy, csc_in_policy, is applied to the outside interface and uses the csc_in access list to ensure that requests for SMTP and HTTP originating on the outside interface and destined for the DMZ network are scanned by the CSC SSM. Scanning HTTP requests protects the web server from HTTP file uploads.

Example 23-1 Service Policies for a Common CSC SSM Scanning Scenario

```
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
hostname(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

hostname(config)# class-map csc_outbound_class
hostname(config-cmap)# match access-list csc_out

hostname(config-cmap)# policy-map csc_out_policy
hostname(config-pmap)# class csc_outbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config-pmap-c)# service-policy csc_out_policy interface inside

hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80
```

```
hostname(config)# class-map csc_inbound_class
hostname(config-cmap)# match access-list csc_in

hostname(config-cmap)# policy-map csc_in_policy
hostname(config-pmap)# class csc_inbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config-pmap-c)# service-policy csc_in_policy interface outside
```

Note FTP inspection must be enabled for the CSC SSM to scan files transferred by FTP. FTP inspection is enabled by default.

Checking SSM Status

To check the status of an SSM, use the **show module** command.

The following is sample output from the **show module** command on an adaptive security appliance with a CSC SSM installed. The Status field indicates the operational status of the SSM. An SSM operating normally has a status of "Up" in the output of the **show module** command. While the adaptive security appliance transfers an application image to the SSM, the Status field in the output reads "Recover." For more information about possible statuses, see the entry for the **show module** command in the *Cisco Security Appliance Command Reference.*

```
hostname# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
 0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000034
 1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         0

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
0 000b.fcf8.c30d to 000b.fcf8.c311  1.0      1.0(10)0     7.1(0)1
1 000b.fcf8.012c to 000b.fcf8.012c  1.0      1.0(10)0     Trend Micro InterScan
                                                          Security Module Version 5.0

Mod SSM Application Name           SSM Application Version
--- ------------------------------ --------------------------
 1 Trend Micro InterScan Security Version 5.0

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
 0 Up Sys              Not Applicable
 1 Up                  Up
```

The argument **1**, at the end of the command, is the slot number occupied by the SSM. If you do not know the slot number, you can omit it and see information about all modules, including the adaptive security appliance, which is considered to occupy slot 0 (zero).

Use the **details** keyword to view additional information for the SSM.

The following is sample output from the **show module details** command on an adaptive security appliance with a CSC SSM installed.

```
hostname# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
```

```
Hardware version:   1.0
Serial Number:      0
Firmware version:   1.0(10)0
Software version:   Trend Micro InterScan Security Module Version 5.0
App. name:          Trend Micro InterScan Security Module
App. version:       Version 5.0
Data plane Status:  Up
Status:             Up
HTTP Service:       Up
Mail Service:       Up
FTP Service:       Up
Activated:          Yes
Mgmt IP addr:       10.23.62.92
Mgmt web port:      8443
```

Transferring an Image onto an SSM

For an intelligent SSM, such as the AIP SSM or CSC SSM, you can transfer application images from a TFTP server to the SSM. This process supports upgrade images and maintenance images.

Note If you are upgrading the application on the SSM, the SSM application may support backup of its configuration. If you do not back up the configuration of the SSM application, it is lost when you transfer an image onto the SSM. For more information about how the SSM supports backups, see the documentation for the specified SSM.

To transfer an image onto an intelligent SSM, perform the following steps:

Step 1 Create or modify a recovery configuration for the SSM.

a. Determine if there is a recovery configuration for the SSM. Use the **show module** command with the **recover** keyword:

```
hostname# show module slot recover
```

where *slot* is the slot number occupied by the SSM.

If the **recover** keyword is not valid, a recovery configuration does not exist. This keyword is available only when a recovery configuration exists for the SSM.

Note When the adaptive security appliance operates in multiple context mode, the **configure** keyword is available only in the system context.

If a recovery configuration exists for the SSM, the adaptive security appliance displays it. Examine the recovery configuration closely to ensure that it is correct, particularly the Image URL field. The following is sample output from the **show module recover** command for an SSM in slot 1.

```
hostname# show module 1 recover
Module 1 recover parameters. . .
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask:          255.255.255.0
Gateway IP Address:  10.1.2.254
```

b. To create or modify the recovery configuration, use the **hw-module module recover** command with the **configure** keyword:

```
hostname# hw-module module slot recover configure
```

where *slot* is the slot number occupied by the SSM.

- Complete the prompts as applicable. If you are modifying a configuration, you can keep the previously configured value by pressing **Enter**. The following example shows the prompts. For more information about them, see the entry for the **hw-module module recover** command in the *Cisco Security Appliance Command Reference.*

```
Image URL [tftp://0.0.0.0/]:
Port IP Address [0.0.0.0]:
VLAN ID [0]:
Gateway IP Address [0.0.0.0]:
```

Note Be sure the TFTP server you specify can transfer files up to 60 MB in size. Also, be sure the TFTP server can connect to the management port IP address that you specify for the SSM.

After you complete the series of prompts, the adaptive security appliance is ready to transfer the image that it finds to the SSM at the specified URL.

Step 2 To transfer the image from the TFTP server to the SSM and restart the SSM, use the **hw-module module recover** command with the **boot** keyword:

```
hostname# hw-module module slot recover boot
```

where *slot* is the slot number occupied by the SSM.

Step 3 Check the progress of the image transfer and SSM restart process with the **show module** command. For details, see the "Checking SSM Status" section on page 23-18.

When the adaptive security appliance completes the image transfer and restarts the SSM, the newly transferred image is running.

Note If the SSM supports configuration backups and you want to restore the configuration of the application running on the SSM, see the documentation of the specified SSM for details.