Managing the AIP SSM and CSC SSM

The Cisco ASA 5500 series adaptive security appliance supports a variety of SSMs. This chapter describes how to configure the adaptive security appliance to support an AIP SSM or a CSC SSM, including how to send traffic to these SSMs.

For information about the 4GE SSM for the ASA 5000 series adaptive security appliance, see Chapter 4, "Configuring Ethernet Settings and Subinterfaces".

Note The Cisco PIX 500 series security appliances does not support SSMs.

This chapter includes the following sections:

Managing the AIP SSM

This section contains the following topics:

About the AIP SSM

The ASA 5500 series adaptive security appliance supports the AIP SSM, which runs advanced IPS software that provides further security inspection. The adaptive security appliance diverts packets to the AIP SSM just before the packet exits the egress interface (or before VPN encryption occurs, if configured) and after other firewall policies are applied. For example, packets that are blocked by an access list are not forwarded to the AIP SSM.

The AIP SSM can operate in one of two modes, as follows:

- **Inline mode**—Places the AIP SSM directly in the traffic flow. No traffic 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 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. You specify this mode with the **inline** keyword of the **ips** command.
- **Promiscuous mode**—Sends a duplicate stream of traffic to the AIP SSM. This mode is less secure, but has little impact on traffic throughput. Unlike operation in inline mode, the SSM operating in promiscuous mode 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 block it. You specify this mode with the **inline** keyword of the **ips** command.

You can specify how the adaptive security appliance treats traffic when the AIP SSM is unavailable due to hardware failure or other causes. Two keywords of the **ips** command control this behavior. 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.

For more information about configuring the operating mode of the AIP SSM and how the adaptive security appliance treats traffic during an AIP SSM failure, see the "Diverting Traffic to the AIP SSM" section on page 19-2.

Getting Started with the AIP SSM

Configuring the AIP SSM is a two-part process that involves configuration of the ASA 5500 series adaptive security appliance first, and then configuration of the AIP SSM:

1. On the ASA 5500 series adaptive security appliance, identify traffic to divert to the AIP SSM (as described in the "Diverting Traffic to the AIP SSM" section on page 19-2).
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. Because the IPS software that runs on the AIP SSM is very robust and 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

Diverting Traffic to the AIP SSM

You use MPF commands to configure the adaptive security appliance to divert traffic to the AIP SSM. Before configuring the adaptive security appliance to do so, read Chapter 18, "Using Modular Policy Framework," which introduces MPF concepts and common commands.

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

Step 1 Create an access list that matches all traffic:

```
hostname(config)# access-list acl-name permit ip any any
```

Step 2 Create a class map to identify the traffic that should be diverted to the AIP SSM. Use the **class-map** command to do so, as follows:

```
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
```

Step 4 Create a policy map or modify an existing policy map that you want to use to send traffic to the AIP SSM. To do so, use the **policy-map** command, as follows.

```
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 Assign the traffic identified by the class map as traffic to be sent to the AIP SSM. Use the **ips** command to do so, as follows.

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

The **inline** and **promiscuous** keywords control the operating mode of the AIP SSM. The **fail-close** and **fail-open** keywords control how the adaptive security appliance treats traffic when the AIP SSM is unavailable. For more information about the operating modes and failure behavior, see the "About the AIP SSM" section on page 19-1.

Step 7 Use the **service-policy** command to apply the policy map globally or to a specific interface, as follows:

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

where *policy_map_name* is the policy map you configured in Step 4. If you want to apply the policy map to traffic on all the interfaces, use the **global** keyword. If you want 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 AIP SSM as specified.

The following example diverts all IP traffic to the AIP SSM in promiscuous mode, and blocks all IP traffic should the AIP SSM card fail 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-ids-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
```

Sessioning to the AIP SSM and Running Setup

After you have completed configuration of the ASA 5500 series adaptive security appliance to divert traffic to the AIP SSM, session to the AIP SSM and run the setup utility for initial configuration.

Note You can either session to the SSM from the adaptive security appliance (by using the **session 1** command) or you can connect directly to the SSM using SSH or Telnet on its management interface. Alternatively, you can use ASDM.

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

Step 1 Enter the **session 1** command to session from the ASA 5500 series adaptive security appliance to the AIP SSM:

```
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 are both **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 dictionary word.

```
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.

Step 3 Enter the **setup** command to run the setup utility for initial configuration of the AIP SSM:

```
AIP SSM# setup
```

You are now ready to configure the AIP SSM for intrusion prevention. See the following URL for AIP SSM configuration information:

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

Managing the CSC SSM

This section contains 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. It accomplishes this by scanning the FTP, HTTP, POP3, and SMTP traffic that you configure the adaptive security appliance to send to it.

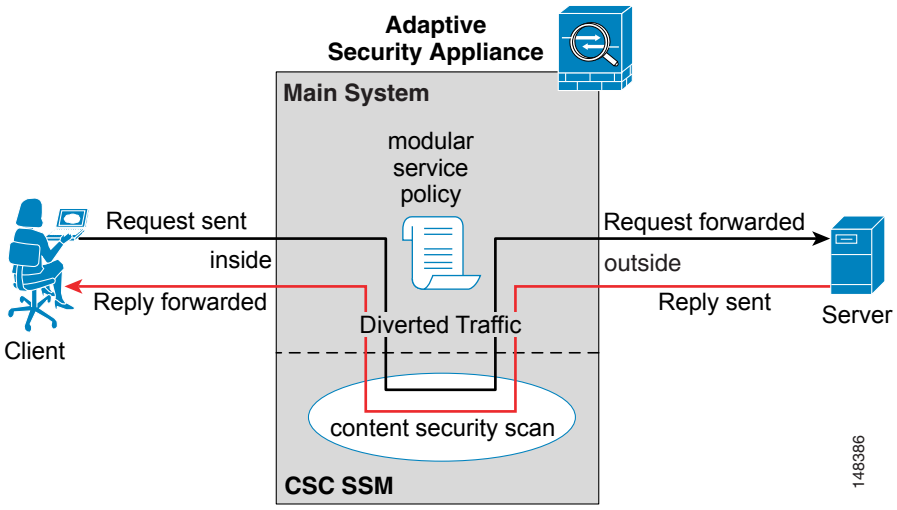
Figure 19-1 illustrates the flow of traffic through an adaptive security appliance that has the following:

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

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 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 19-1 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. Use of the CSC SSM GUI is explained in the *Cisco Content Security and Control SSM Administrator Guide*.

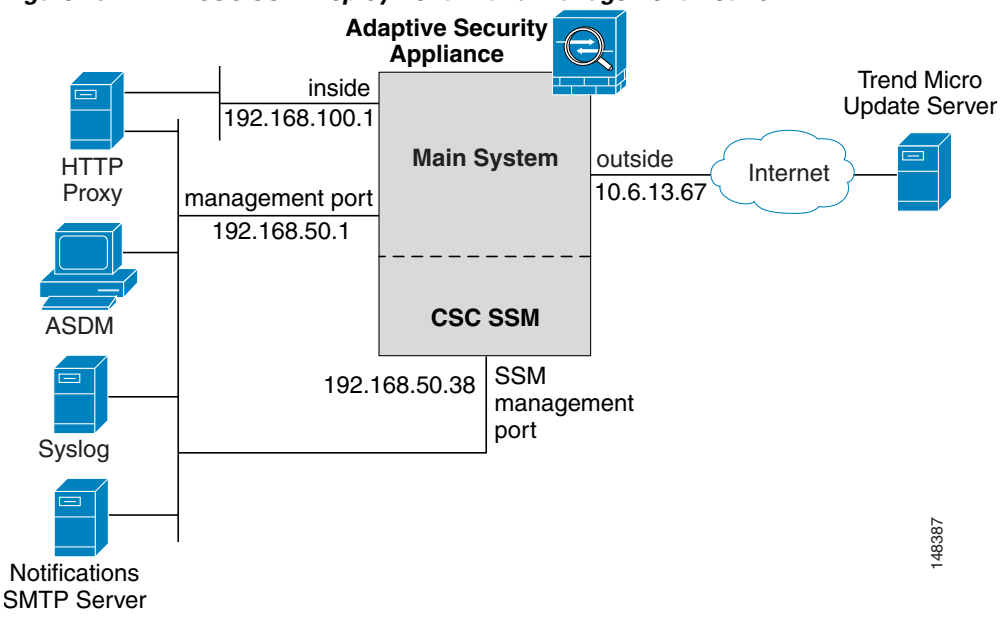
Note ASDM and the CSC SSM maintain separate passwords. You can configure their passwords to be identical; however, changing one of these two passwords does not affect the other password.

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 19-2 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 in Figure 19-2 are the following:

- An HTTP proxy server is connected to the inside network and to the management network. This 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 email notifications for the CSC SSM and a syslog server that the CSC SSM can send syslog messages to.

Figure 19-2 CSC SSM Deployment with a Management Network



CSC SSM cannot suport stateful failover, because the CSC SSM does not maintain connection information and therefore cannot provide the failover unit with information necessary for stateful failover. The connections that a CSC SSM is scanning are dropped upon failure of the security appliance that the CSC SSM is installed in. When the standby adaptive security appliance becomes active, it will forward the scanned traffic to its 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 simple 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 email notifications and syslogging.

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 email. 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.
- SSM management port IP address, netmask, and gateway IP address.

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

- DNS server IP address.
- HTTP proxy server IP address (required only if your security policies require use of a proxy server for HTTP access to the Internet).
- Domain name and hostname for the SSM.
- An email address and an SMTP server IP address and port number, for email 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 that the CSC SSM is in.

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 33-4.

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 In ASDM, run the Content Security setup wizard. To do so, access the ASDM GUI in a supported web browser and on the Home page, click the **Content Security** tab. The Content Security setup wizard runs. For assistance with the Content Security 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 (as described in the "Diverting Traffic to the CSC SSM" section on page 19-11).

Step 8 (Optional) Review the default content security policies in the CSC SSM GUI. The default content security policies are suitable for most implementations. Modifying them is advanced configuration that you should perform only after reading the *Cisco Content Security and Control 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 purchased. By default, all features included in the license you 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 blue 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. It supports these protocols only when the destination port of the packet requesting the connection is the well known port for the protocol, that is, 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 email, you would not want to configure the adaptive security appliance to divert POP3 traffic to the CSC SSM (you would want to block it instead).

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.

The action of scanning traffic with the CSC SSM is enabled with the **csc** command, which must be part of a service policy. Service policies can be applied globally or to specific interfaces; therefore, you can choose to 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 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. This 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 if the class map for the policy identifies traffic for scanning, the adaptive security appliance diverts it to the CSC SSM.

However, bi-directionality means that if you divert to the CSC SSM any of the supported traffic types that cross a given interface, the CSC SSM is likely performing needless 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 such traffic to the CSC SSM.

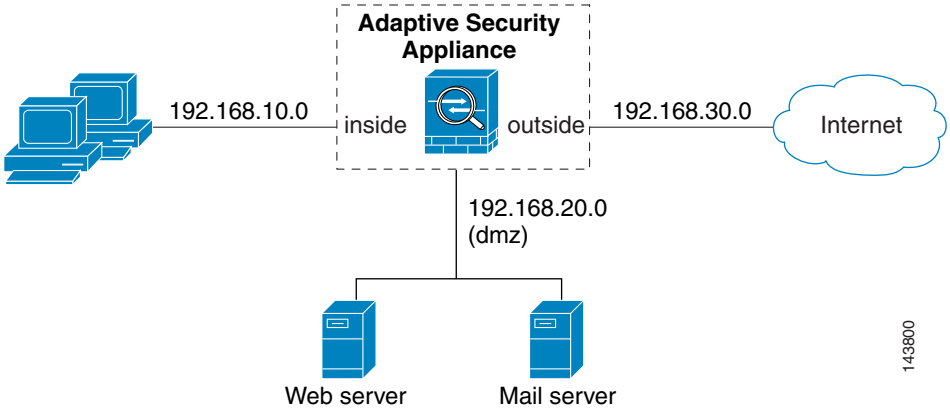
Therefore, we highly recommend using access lists to further limit the traffic selected by the class maps of CSC SSM service policies. Specifically, use access lists that match the following:

- 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 19-3, 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 19-3 Common Network Configuration for CSC SSM Scanning



There are many ways you could configure the adaptive security appliance to identify the traffic that you want to scan. 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 could 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, but 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 uses 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. It simply exempts the traffic from being matched by the policy map and thus prevents the adaptive security appliance from sending it to the CSC SSM.

You can use deny statements in an access list to exempt connections with trusted external hosts 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 such a site had 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 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 email would be diverted to the CSC SSM for scanning. It 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 complete example service policy configuration using the access lists in this section, see Example 19-1.

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 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.

Use of the **set connection** command to protect the CSC SSM and the destinations of connections it scans is included in the "Diverting Traffic to the CSC SSM" section on page 19-11.

Diverting Traffic to the CSC SSM

You use MPF commands to configure the adaptive security appliance to divert traffic to the CSC SSM. Before configuring the adaptive security appliance to do so, read Chapter 18, "Using Modular Policy Framework," which introduces MPF 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. To do so, use the **access-list extended** command. Create as many ACEs as needed to match all the traffic. For example, if you want to specify FTP, HTTP, POP3, and SMTP traffic, you would need four ACEs. For guidance on identifying the traffic you want to scan, see the "Determining What Traffic to Scan" section on page 19-9.

Step 2 Create a class map to identify the traffic that should be diverted to the CSC SSM. Use the **class-map** command to do so, as follows.

```
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
```

Step 4 Create a policy map or modify an existing policy map that you want to use to send traffic to the CSC SSM. To do so, use the **policy-map** command, as follows.

```
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 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. Use the **csc** command to do so, as follows.

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

The **fail-close** and **fail-open** keywords control how the adaptive security appliance treats 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 19-5.

Step 8 Use the **service-policy** command to apply the policy map globally or to a specific interface, as follows:

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

where *policy_map_name* is the policy map you configured in Step 4. If you want to apply the policy map to traffic on all the interfaces, use the **global** keyword. If you want 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 19-1 is based on the network shown in Figure 19-3. It creates 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 19-1 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)# policy-map csc_out_policy
hostname(config-pmap)# class csc_outbound_class
hostname(config-pmap-c)# csc fail-close

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

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

Note FTP inspection must be enabled for 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 follow example output is from 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.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         JAB100301NE

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 0015.c6fa.2c0f to 0015.c6fa.2c0f  1.0          1.0(10)0     CSC SSM 6.0 (Build#1349)

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CSC SSM                        Down             6.0 (Build#1349)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  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 follow example output is from 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:      JAB100301NE
Firmware version:   1.0(10)0
Software version:   CSC SSM 6.0 (Build#1349)
MAC Address Range:  0015.c6fa.2c0f to 0015.c6fa.2c0f
App. name:          CSC SSM
App. Status:        Up
App. Status Desc:   CSC SSM scan services are available
App. version:       6.0 (Build#1349)
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
Peer IP addr:       <not enabled>
```

Transferring an Image onto an SSM

For an intelligent SSM, such as 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 your SSM supports backups, see the documentation for your SSM.

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

Step 1 Create or modify a recovery configuration for the SSM. To do so, perform the following steps:

a. Determine if there is a recovery configuration for the SSM. To do so, use the **show module** command with the **recover** keyword, as follows.

```
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. The **recover** keyword of the **show module** command 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 there is a recovery configuration for the SSM, the adaptive security appliance displays it. Examine the recovery configuration closely to ensure that it is correct, especially the Image URL field. The following example show a recovery configuration 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/csc-img
Port IP Address:     10.1.2.10
Port Mask :          255.255.255.0
Gateway IP Address:  10.1.2.254
```

b. If you need to create or modify the recovery configuration, use the **hw-module module recover** command with the **configure** keyword, as follows:

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

Step 2 Transfer the image from the TFTP server to the SSM and restart the SSM. To do so, use the **hw-module module recover** command with the **boot** keyword, as follows.

```
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. To do so, use the **show module** command. For details, see the "Checking SSM Status" section on page 19-13.

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

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