CHAPTER 60

Configuring the Content Security and Control Application on the CSC SSM

This chapter describes how to configure the Content Security and Control (CSC) application that is installed in a CSC SSM in the ASA.

The chapter includes the following sections:

Information About the CSC SSM

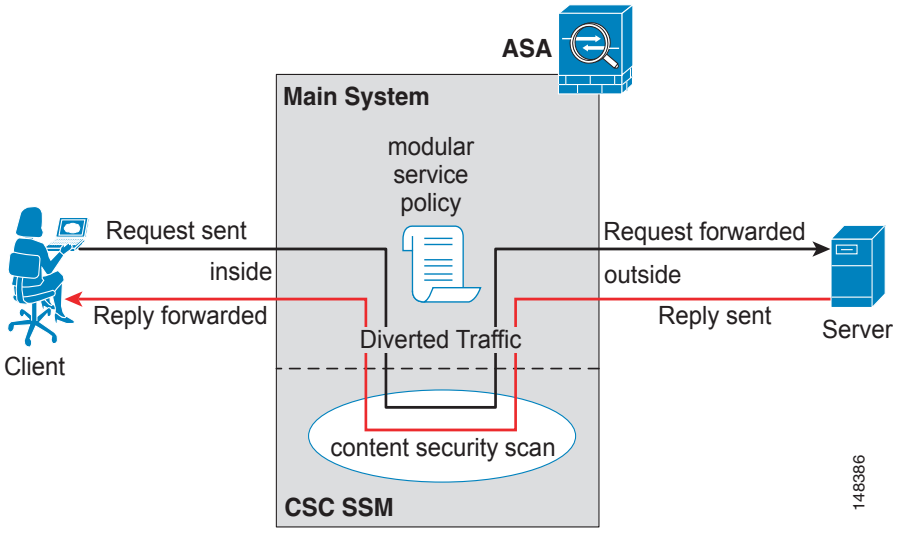
The ASA 5500 series ASA supports the CSC SSM, which runs Content Security and Control software. The CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic by scanning the FTP, HTTP, POP3, and SMTP packets that you configure the ASA to send to it.

Figure 60-1 shows the flow of traffic through an ASA 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 ASA to scan traffic sent from the outside to SMTP servers protected by the ASA.

Figure 60-1 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.

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 ASA is made through a management port on the ASA. 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 ASA management port and the SSM management port.

Figure 60-2 shows an ASA 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. In this configuration, the following items are of particular interest:

- 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 ASA is connected to the management network. To allow management of the ASA 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 syslog messages.

Figure 60-2 CSC SSM Deployment with a Management Network

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 ASA to divert POP3 traffic to the CSC SSM. Instead, block this traffic.

To maximize performance of the ASA and the CSC SSM, divert only the traffic to the CSC SSM that you want the CSC SSM to scan. Diverting traffic that you do not want scanned, such as traffic between a trusted source and destination, can adversely affect network performance.

Based on the configuration shown in Figure 60-3, configure the ASA to divert to the CSC SSM only 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. Exclude from scanning HTTP requests from the inside network to the web server on the DMZ network.

Figure 60-3 Common Network Configuration for CSC SSM Scanning

Licensing Requirements for the CSC SSM

The following table shows the licensing requirements for this feature:

Model	License Requirement
ASA 5510	• Base License—Supports SMTP virus scanning, POP3 virus scanning and content filtering, web mail virus scanning, HTTP file blocking, FTP virus scanning and file blocking, logging, and automatic updates. Supports two contexts. *Optional licenses: 5 contexts.* • Security Plus License—Supports the Base license features, plus SMTP anti-spam, SMTP content filtering, POP3 anti-spam, URL blocking, and URL filtering. Supports two contexts. *Optional license: 5 contexts.*
ASA 5520	Base License—Supports all features. Supports two contexts. *Optional licenses: 5, 10, or 20 contexts.*
ASA 5540	Base License—Supports all features. Supports two contexts. *Optional licenses: 5, 10, 20, or 50 contexts.*
All other models	No support.

Prerequisites for the CSC SSM

The CSC SSM has the following prerequisites:

- A CSC SSM card must be installed in the ASA.
- A Product Authorization Key (PAK) for use in registering the CSC SSM.
- Activation keys that you receive by e-mail after you register the CSC SSM.
- The management port of the CSC SSM must be connected to your network to allow management and automatic updates of the CSC SSM software.
- The CSC SSM management port IP address must be accessible by the hosts used to run ASDM.
- You must obtain the following information to use in configuring the CSC SSM:
  - The CSC SSM management port IP address, netmask, and gateway IP address.
  - 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 that are allowed to manage the CSC SSM. The IP addresses for the CSC SSM management port and the ASA management interface can be in different subnets.
  - Password for the CSC SSM.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context modes.

Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

Failover Guidelines

Does not support sessions in Stateful Failover. The CSC SSM does not maintain connection information, and therefore cannot provide the failover unit with the required information. The connections that a CSC SSM is scanning are dropped when the ASA in which the CSC SSM is installed fails. When the standby ASA becomes active, it forwards the scanned traffic to the CSC SSM and the connections are reset.

IPv6 Guidelines

Does not support IPv6.

Model Guidelines

Supported on the ASA 5510, ASA 5520, and ASA 5540 only.

Default Settings

Table 60-1 lists the default settings for the CSC SSM.

Table 60-1 Default CSC SSM Parameters

Parameter	Default
FTP inspection on the ASA	Enabled
All features included in the license(s) that you have purchased	Enabled

Configuring the CSC SSM

This section describes how to configure the CSC SSM, and includes the following topics:

- Before Configuring the CSC SSM, page 60-6
- Diverting Traffic to the CSC SSM, page 60-7

Before Configuring the CSC SSM

Before configuring the ASA and the CSC SSM, perform the following steps:

Step 1 If the CSC SSM did not come pre-installed in a Cisco ASA 5500 series ASA, install it and connect a network cable to the management port of the SSM. For assistance with installation and connecting the SSM, see the "Additional References" section on page 60-11.

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 syslog messages.

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

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

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

Step 3 Obtain the following information for use in Step 6:

- Activation keys
- The CSC SSM management port IP address, netmask, and gateway IP address
- 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 ASA in which the CSC SSM is installed.

Note If you are accessing ASDM for the first time, see the "Additional References" section on page 60-11.

For more information about enabling ASDM access, see the "Allowing HTTPS Access for ASDM" section on page 37-4.

Step 5 Verify time settings on the ASA. Time setting accuracy is important for logging of security events and for automatic updates of CSC SSM software. Do one of the following:

- 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 Access the ASDM GUI in a supported web browser and in the Home pane, click the **Content Security** tab.

Step 7 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.

Step 8 On the ASA 5500 series ASA, identify traffic to divert to the CSC SSM. For instructions, see the "Diverting Traffic to the CSC SSM" section on page 60-7.

Step 9 (Optional) Review the default content security policies in the CSC SSM GUI, which are suitable for most implementations. You review the content security policies by viewing the enabled features in the CSC SSM GUI. For the availability of features, see the "Licensing Requirements for the CSC SSM" section on page 60-4. For the default settings, see the "Default Settings" section on page 60-6.

To access the CSC SSM GUI, in ASDM choose **Configuration > Trend Micro Content Security**, and then click one of the following: **Web**, **Mail**, **File Transfer**, or **Updates**.

Diverting Traffic to the CSC SSM

You use Modular Policy Framework commands to configure the ASA to divert traffic to the CSC SSM.

Prerequisites

Before configuring the ASA to divert traffic to the CSC SSM, see Chapter 9, "Using Modular Policy Framework," which introduces Modular Policy Framework concepts and common commands.

Detailed Steps

	Command	Purpose
Step 1	**access-list extended** **Example:** `hostname(config)# access-list extended`	Creates an access list that matches the traffic you want scanned by the CSC SSM. 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 that you want to scan, see the "Diverting Traffic to the CSC SSM" section on page 60-7.
Step 2	**class-map** *class_map_name* **Example:** `hostname(config)# class-map class_map_name`	Creates a class map to identify the traffic that should be diverted to the CSC SSM. The *class_map_name* argument is the name of the traffic class. When you enter the **class-map** command, the CLI enters class map configuration mode.
Step 3	**match access-list** *acl-name* **Example:** `hostname(config-cmap)# match access-list acl-name`	Identifies the traffic to be scanned with the access list that you created in Step 1. The *acl-name* argument is the name of the access list.
Step 4	**policy-map** *policy_map_name* **Example:** `hostname(config-cmap)# policy-map policy_map_name`	Creates a policy map or modify an existing policy map that you want to use to send traffic to the CSC SSM. The *policy_map_name* argument is the name of the policy map. When you enter the **policy-map** command, the CLI enters policy map configuration mode.
Step 5	**class** *class_map_name* **Example:** `hostname(config-pmap)# class class_map_name`	Specifies the class map, created in Step 2, that identifies the traffic to be scanned. The *class_map_name* argument is the name of the class map that you created in Step 2. The CLI enters the policy map class configuration mode.
Step 6	**set connection per-client-max** *n* **Example:** `hostname(config-pmap-c)# set connection per-client-max 5`	Lets you configure limits to thwart DoS attacks. The **per-client-max** parameter limits the maximum number of connections that individual clients can open. If a client uses more network resources simultaneously than is desired, you can enforce a per-client limit for simultaneous connections that the ASA diverts to the CSC SSM. The *n* argument is the maximum number of simultaneous connections that the ASA allows 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.

	Command	Purpose
Step 7	**csc** {**fail-close** | **fail-open**} **Example:** `hostname(config-pmap-c)# csc {fail-close | fail-open}`	Enables traffic scanning with the CSC SSM and assigns the traffic identified by the class map as traffic to be sent to the CSC SSM. Must be part of a service policy, which can be applied globally or to specific interfaces. Ensures that all unencrypted connections through the ASA are scanned by the CSC SSM; however, this setting may mean that traffic from trusted sources is needlessly scanned. If enabled in interface-specific service policies, this command is bi-directional. Bi-directionality means that when the ASA opens a new connection, if this 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 ASA 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. Therefore, to further limit the traffic selected by the class maps of CSC SSM service policies, we recommend using access lists that match the following: • HTTP connections to outside networks. • FTP connections from clients inside the ASA to servers outside the ASA. • POP3 connections from clients inside the security appliance to servers outside the ASA. • Incoming SMTP connections destined to inside mail servers. The **fail-close** and **fail-open** keywords control how the ASA handles traffic when the CSC SSM is unavailable. For more information about the operating modes and failure behavior, see the "Guidelines and Limitations" section on page 60-5.
Step 8	**service-policy** *policy_map_name* [**global** | **interface** *interface_ID*] **Example:** `hostname(config-pmap-c)# service-policy policy_map_name [global | interface interface_ID]`	Applies the policy map globally or to a specific interface. The *policy_map_name* argument is the policy map that 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.

Monitoring the CSC SSM

For information about how to monitor the CSC SSM, see the "Monitoring SSMs and SSCs" section on page 58-9.

Configuration Examples for the CSC SSM

To identify the traffic that you want to scan, you can configure the ASA in different ways. One approach is to define two service policies, one on the inside interface and one on the outside interface, each with an access list that matches traffic to be scanned. The following example is based on the network shown in Figure 60-3 and shows the creation of two service policies for a common CSC SSM scanning scenario:

- 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.

```
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
```

The following example shows how to use an access list to exempt the traffic from being matched by the policy map and prevent the ASA from sending traffic to the CSC SSM:

```
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
```

The following example shows how to add an 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:

```
hostname(config)# 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 following example shows how to use the access list on the service policy applied to the outside interface:

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

The following example shows how to add an ACE to the csc_in access list to use the CSC SSM to protect the web server on a DMZ network from infected files uploaded by HTTP from external hosts:

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

Additional References

For additional information related to implementing the CSC SSM, see the following documents:

Related Topic	Document Title
Instructions on use of the CSC SSM GUI. Additional licensing requirements of specific windows available in the CSC SSM GUI. Reviewing the default content security policies in the CSC SSM GUI before modifying them or entering advanced configuration settings.	*Trend Micro InterScan for Cisco CSC SSM Administrator Guide*
Accessing ASDM for the first time and assistance with the Startup Wizard.	*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
Assistance with SSM hardware installation and connection to the ASA.	*Cisco ASA 5500 Series Hardware Installation Guide*
Technical Documentation, Marketing, and Support-related information	See the following URL: http://www.cisco.com/en/US/products/ps6823/index.html.

Feature History for the CSC SSM

Table 60-2 lists the release history for this feature.

Table 60-2 Feature History for the CSC SSM

Feature Name	Releases	Feature Information
CSC SSM	7.0(1)	The CSC SSM runs Content Security and Control software, which provides protection against viruses, spyware, spam, and other unwanted traffic. The following commands were introduced: • **csc {fail-close | fail-open}** • **hw-module module 1** [**recover | reload | reset | shutdown**] • **session** • **show module** [**all** | *slot* [**details | recover**]]
Password reset	7.2(2)	The **hw-module module password-reset** command was introduced.
CSC SSM	8.1(1), 8.1(2)	This feature is not supported.