Sizing Guide
Cisco ASA 5500 Series CSC-SSM

This guide is intended to assist customers with sizing deployments of the Cisco® ASA 5500 Series Content Security and Control Security Services Module (CSC-SSM). This guide should be used to choose the appropriate type of module and number of user licenses to best protect the Internet gateway and client systems.

Product Overview

The Cisco ASA 5500 Series CSC-SSM integrates into a wide assortment of networking environments and operates efficiently under typical network traffic conditions. For example, most employees browse the Internet more frequently than they download electronic mail. Thus, the CSC-SSM allocates more of its resources to scanning HTTP traffic. However, the computing resources available to the CSC-SSM are finite. Customers that have atypical networking environments should use this guide to choose the appropriate type of module and number of user licenses that will best protect their endpoints.

User License Sizing Guidelines

As stated in the CSC-SSM End User License Agreement, the module's user licenses are not for simultaneous users—they are for the total number of users whose traffic is being scanned by the module. Customers should therefore size their user licenses for the total number of employees protected by the CSC-SSM.

Module Sizing Guidelines

Cisco recommends that customers license the appropriate CSC-SSM configuration by sizing their environment in two ways: by the number of IP connections, or by the network traffic mix. A connection is defined as an IP-to-IP and port-to-port mapping.

Number of IP Connections

This refers to the number of simultaneous IP connections flowing through the CSC-SSM. The protocols that the module inspects (HTTP, FTP, POP3, and SMTP) are not "always on". Instead, they are intermittent and periodically activated when a user attempts to browse a Website, download a file, retrieve electronic mail, etc. The CSC-SSM takes advantage of the intermittent nature of these protocols to efficiently utilize the available resources. The standardized technique it uses is called "statistical multiplexing". The CSC-SSM-10 has a hardware limitation of 500 simultaneous IP connections, while CSC-SSM-20 supports 1000 connections (regardless of number of users generating them).

Network Traffic Mix

In a typical midsize enterprise, the majority of the traffic is Internet access (HTTP); this often exceeds 80 percent of total traffic volume, while electronic mail (SMTP, POP3) and other data traffic (FTP) is a minor portion of the mix. The CSC-SSM allocates its resources according to this profile so that the traffic that endpoints generate is protected efficiently. Organizations that use electronic mail to send numerous large attachments (10 MB+) to

broad distribution lists may exceed the number of simultaneous connections that the CSC-SSM allocates to the SMTP and POP3 protocols. For reference, the CSC-SSM-10 supports 45 simultaneous connections and the CSC-SSM-20 supports 75; in both cases, the module is able to queue an additional 128 connections.

The CSC-SSM devotes a large number of simultaneous connections to HTTP because it is the most frequently used protocol. For the vast majority of networking environments, the 500 connections of the CSC-SSM-10 and the 1000 connections of the CSC-SSM-20, along with a queue of 128, are more than enough. In unusual situations where employees spend much of their time browsing Websites, the number of connections may not be enough and an upgrade to a larger CSC-SSM may be in order. As a rule, both Internet Explorer and Firefox/Netscape Web browsers will open two simultaneous HTTP connections; however, users can easily change those settings. Please keep this in mind when budgeting your HTTP needs.

The final protocol that the CSC-SSM supports is FTP. This is the least likely to be used in the average customer environment. However, each FTP download requires several simultaneous connections for control transactions and file downloads. Therefore, the CSC-SSM-10 is equipped to handle 50 simultaneous FTP connections and the CSC-SSM-20 can handle 100, again with a queue of 128. The number of connections is only likely to be exceeded in situations where the CSC-SSM is protecting dedicated FTP servers.

Customers that have already deployed one or more Cisco ASA devices can use the following commands on the Cisco ASA 5500 console to determine how many established connections exist:

- HTTP—**show conn fport 80**
- SMTP—**show conn lport 25**
- POP3—**show conn lport 110**
- FTP Control—**show conn fport 21**
- FTP Data—**show conn fport 20**

Customers that regularly exceed the number of IP or protocol connections should consider upgrading to a higher-capacity CSC-SSM if possible. If an upgrade is not possible, customers should consider implementation of Trend Micro's standalone software or dedicated appliances.

Note: A connection is simply a TCP connection. For example, in a typical normal-mode FTP session there are two connections involved: the control connection, which has a server side port equal to 21, and a data connection for file download with a server side port of 20. In the case of HTTP, browsers usually open multiple connections to increase the speed at which the elements on the page download. For example, when browsing to http://www.cisco.com, the browser will open one connection to download the index page and parse it, and then it opens up to two simultaneous connections to download the hyperlinks such as pictures or animation.

CISCO

Printed in USA

C07-383605-02   09/13