Cisco ASA 5500 Series Content Security and Control Security Services Module

General information

Q. What is the Cisco® ASA 5500 Series Content Security and Control Security Service Module (CSC-SSM)?

A. The Cisco ASA 5500 Series CSC-SSM is an add-on services module for Cisco ASA 5500 Series appliances. It delivers industry-leading threat protection and content control at the Internet edge, providing comprehensive antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, URL blocking and filtering, and content filtering services.

Q. What are the advantages of the Cisco ASA 5500 Series CSC-SSM?

A. Previously, in order to take advantage of Cisco's market-leading firewall and VPN services and Trend Micro's industry-leading gateway antivirus and content security solution, customers had to purchase two separate products from Cisco and Trend Micro, respectively. The Cisco CSC-SSM, together with the Cisco ASA 5500 Series purpose-built appliances, combines these market-leading products into a comprehensive unified threat prevention solution, in a single easily deployable and manageable package.

Q. What are the main features of the Cisco ASA 5500 Series CSC-SSM?

A. The Cisco ASA 5500 Series CSC -SSM provides the following elements:

- Comprehensive malware protection—Incorporates Trend Micro's award-winning antivirus and anti-spyware technologies. The CSC-SSM can prevent virtually all known malicious code from entering and propagating across the network. This helps prevent disruption of business-critical applications and services, protect valuable key systems, prevent employee downtime, and reduce the costly process of cleaning up after an infection.
- Advanced content filtering—Integrates URL filtering, content filtering, and anti-phishing technology to help protect the business and individual employees from the theft of confidential information and to reduce potential legal liabilities associated with content in violation of network use policies. The module can help businesses comply with network content regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and the Data Protection Act.
- Integrated message security—Integrates anti-spam technology that removes the vast majority of unsolicited e-mail before it gets to the mail server, increasing employee productivity and preventing wastage of valuable network bandwidth and storage resources.

- Customization and tuning capabilities—Provides administrators with the ability to customize control over spam and content functions to suit specific corporate policies or network environments.
- Ease of management and automatic update capabilities—Ships with intelligent default settings and an intuitive interface integrated with the Cisco Adaptive Security Device Manager (ASDM) to ease initial configuration, deployment, and ongoing operations. Automatic updates of all CSC-SSM components, including scanning engines and pattern files, ensures that the network is always protected against the latest threats with minimal administrative effort.

Q. What models are available?

A. There are two available models—the CSC-SSM-10 and CSC-SSM-20. Both models are compatible with the Cisco ASA 5510 and 5520 chassis. The CSC-SSM-10 provides support for organizations with up to 500 users. The CSC-SSM-20 provides support for organizations with up to 1000 users. The Cisco ASA 5540 is a supported platform for both CSC-SSM models, but the 1000-user capacity makes this combination a non-optimal configuration.

Q. What features and services are included with the Cisco ASA 5500 Series CSC-SSM?

A. The Cisco ASA 5500 Series CSC-SSM ships with a default feature set that provides antivirus, anti-spyware, and file blocking services. A premium Plus license is available for additional capabilities, including anti-spam, anti-phishing, URL blocking/filtering, and content control services. These optional feature licenses are available for an additional charge for each CSC-SSM. In addition, organizations can extend the user capacity of the CSC-SSM by purchasing and installing additional user licenses. By default, the CSC-SSM-10 and CSC-SSM-20 models ship with 50 and 500 user licenses, respectively. Several tiers of user license upgrades are available, including 100-, 250-, and 500-user packs for the CSC-SSM-10 and 750- and 1000-user packs for the CSC-SSM-20. Table 1 illustrates the standard and optional licenses available for the CSC-SSM.

Table 1. Standard and Optional Features

CSC-SSM Hardware	Standard Licenses	Optional Licenses	
		User Upgrades (Total Users)	Feature Upgrades
CSC-SSM-10	• 50 users • Antivirus, anti-spyware, file blocking	• 100 users • 250 users • 500 users	• Plus license–Adds anti-spam, anti-phishing, URL blocking/filtering, and content control
CSC-SSM-20	• 500 users • Antivirus, anti-spyware, file blocking	• 750 users • 1000 users	• Plus license–Adds anti-spam, anti-phishing, URL blocking/filtering, and content control

Q. Where do I deploy the Cisco ASA 5500 Series CSC-SSM?

A. The Cisco ASA 5500 Series CSC-SSM and appliances are designed to be deployed at borders between organizations or external networks, such as Internet connection points. By positioning these appliances at the Internet edge, the CSC-SSM sits between your users and the Internet, giving the administrator the ability to select traffic to be scanned by the CSC-SSM appropriately.

Q. What is considered a "user"?

A. A user is an employee, contractor, or other regular worker that is protected by the product. For licensing and legal purposes, the CSC-SSM should be licensed for the total, not concurrent, number of users whose traffic is being scanned.

Q. What type of antivirus protection does the Cisco ASA 5500 Series CSC-SSM offer?

A. The Cisco ASA 5500 Series CSC-SSM provides file-based antivirus protection, which consists of protection against viruses, Trojan horses, malicious code, macros, and other malware. The CSC-SSM operates as a transparent proxy inspecting files and packets as they traverse the ASA 5500 appliance; thus, it is capable of intercepting malicious content before it can harm the intended system. As a result of this mode of operation, the CSC-SSM can also notify users of the removal of suspicious files or content and notify them that this actions were taken and why.

Q. Does the antivirus technology scan compressed files?

A. Yes. It can scan multiple layers of compressed files by decompressing the file, scanning the content, and recompressing the file.

Q. How often is the antivirus signature list updated?

A. Trend Micro's TrendLabs releases one or more regular pattern updates for the Cisco ASA 5500 Series CSC-SSM each week, with emergency official updates delivered more frequently, if necessary, to protect customers from an emerging widespread threat.

Q. How is the Cisco ASA 5500 Series CSC-SSM managed?

A. The Cisco ASA 5500 Series CSC-SSM comes configured with appropriate default settings for most deployments. Setup, management, and monitoring can be carried out through Cisco ASDM, which provides a setup wizard to activate the CSC-SSM and the security policy rules table where the administrator can identify relevant traffic to be scanned by the CSC-SSM.

Q. How do I manage multiple Cisco ASA 5500 Series CSC-SSMs?

A. Multiple CSC-SSM units can be centrally managed using the Trend Micro Control Manager, available as an additional fee option from Trend Micro. The Trend Micro Control Manager can centrally manage multiple CSC-SSMs and other Trend Micro products within the organization. This will provide for consolidated one-stop management of all antivirus and other associated functions and technologies within larger organizations with mixed deployments of multiple CSC-SSMs and Trend Micro products.

Q. What types of attacks does the Cisco ASA 5500 Series CSC-SSM block?

A. The Cisco ASA 5500 Series CSC-SSM uses HTTP, FTP, SMTP, and POP3 protocols to detect and block unauthorized content and malware—including file-based viruses, spyware, directory harvest attacks, spam, and phishing—from entering the network. By stopping malware from reaching desktop or server systems, attacks are stopped before they can start.

Q. Does the Cisco ASA 5500 Series CSC-SSM stop Internet worms?

A. No. For Internet worm mitigation using the Cisco ASA 5500 Series, customers should purchase the Advanced Inspection and Prevention Security Services Module (AIP-SSM), designed for protection of critical assets such as servers, and the optional Cisco Incident Control Server (ICS) product, designed for rapid-response protection against newly emerging worm-based threats.

Q. How does the Cisco ASA 5500 Series CSC-SSM keep up with new vulnerabilities?

A. The Cisco ASA 5500 Series CSC-SSM is backed by Trend Micro's TrendLabs, one of the largest teams of virus, spyware, and spam experts in the industry, working 24 hours a day to ensure that the module is providing the most up-to-date protection. Threat updates are automatically deployed to the CSC-SSM at regular intervals.

Q. Will the Cisco ASA 5500 Series CSC-SSM ever block legitimate traffic?

A. Properly configured, it's highly unlikely that the Cisco ASA 5500 Series CSC-SSM will stop legitimate Internet traffic. Cisco provides detailed configuration options for users to set up the module specifically to the needs of their environment.

Q. What if the module fails for any reason?

A. Cisco ASA 5500 Series appliances can be configured to deny traffic or pass traffic uninspected in case of a CSC-SSM failure. The Cisco ASA also supports failover for the CSC-SSM. If the appliance is a member of a failover group, a CSC-SSM failure will trigger a failover to the standby unit in the pair. Flows that are established and active through the CSC-SSM at the time of failover will have to be re-established.

Support and Miscellaneous

Q. How are technical support, updates, and returns handled?

A. Technical support is provided by the Cisco Technical Assistance Center (TAC) or an authorized Cisco partner. Trend Micro provides support through the Cisco TAC for issues related to the application software on the CSC-SSM. Pattern files and scan engine updates are provided directly and transparently by Trend Micro's update servers. Returns are handled by the company that the customer purchased the module from, just as they would be for all other Cisco products.

Q. How do I purchase a Cisco ASA 5500 Series CSC-SSM?

A. To place an order, please visit the Cisco Ordering Home Page or contact your authorized Cisco reseller or Cisco sales associate.

Q. How do I purchase support? What support options are available for the Cisco ASA 5500 Series CSC-SSM?

A. Service programs comprise hardware support, software support, and content subscription elements. Table 2 lists the service and support contracts offered for the Cisco ASA 5500 Series CSC-SSM. Customers are provided with the first year of the software update service as part of the purchase price of module. For years two and beyond, customers will renew their software and subscription contracts directly through Cisco for an annual fee beginning one year after the time of license registration. Cisco offers SMARTnet® maintenance programs covering technical support and hardware maintenance for the CSC-SSM for an additional annual fee. Both the software update service and the Cisco SMARTnet service are required to maximize the protection and optimal performance of your Cisco ASA 5500 Series CSC-SSM solution.

Table 2. Available Support Services

Support Deliverables	Cisco SMARTnet Service	Software Update Service
Cisco ASA 5500 Series Appliance Chassis Support		
Registered access to Cisco.com	Included	—
Cisco TAC technical support 24x7x365	Included	—
Operating system software releases (maintenance, major, minor)	Included	—
Hardware replacement options	Included	—
Cisco ASA 5500 Series CSC-SSM Support		
Registered access to Cisco.com	Included	—
Cisco TAC technical support 24 x 7 x 365	Included	—
Operating system software releases (maintenance, major, minor)	Included	—
Pattern file, scan engine, and signature updates	—	Included
Hardware replacement options	Included	—

Q. Do I need to purchase both the Cisco SMARTnet and software update services?

A. Yes. Both services are required to ensure that your Cisco ASA 5500 Series CSC-SSM is up to date and operating at optimal performance. The first year of the software update services is included in the purchase price of the product.

Q. If I have a piece of malware (or suspected malware) that Cisco ASA 5500 Series CSC-SSM doesn't catch, how do I submit the suspect data for analysis? Is there a tracking mechanism (along the lines of a TAC case) that tracks the submission and answer?

A. Suspected malware can be submitted for review to http://subwiz.trendmicro.com/SubWiz/Default.asp. You will be notified via e-mail as to the status of your submission. .

Q. How do pattern file updates affect traffic passing through the Cisco ASA 5500 Series CSC-SSM?

A. Updates can be scheduled at times that are appropriate for your business. When a new pattern file or scan engine update is received, the scanning process is restarted and traffic is delayed momentarily while the restart occurs. This does not trigger a failover event, but updates should be scheduled for times of the day with lower traffic volumes.

Q. Does the Cisco ASA 5500 Series CSC-SSM replace the need for desktop or laptop antivirus protection or the Cisco Security Agent?

A. No. The Cisco ASA 5500 Series CSC-SSM is an important part of a multilayer security strategy that also includes intrusion prevention and desktop security. Desktop and laptop security products, such as Trend Micro's OfficeScan and the Cisco Security Agent, provide additional layers of protection from threats that can be introduced directly onto those computers through things like removable media (flash and optical drives, for example) and when the computer is used in less secure environments outside of the corporate network. In addition, OfficeScan and the Cisco Security Agent provide support for Cisco's Network Admission Control (NAC) program, an integral part of preventing endpoints from introducing threats into the network.

Q. Can I use my previously purchased Cisco ASA 5500 Series AIP-SSM card to run the CSC software application?

A. No. The SSM hardware is not interchangeable and Cisco does not support this conversion. The SSM hardware will not run both AIP and CSC applications simultaneously. Interested customers can contact their reseller or sales professional about possible trade-in options.

Q. Can I use other features of the Cisco ASA Series appliances, such as firewall and VPN, simultaneously with CSC-SSM capabilities?

A. Yes. The Cisco ASA 5500 Series CSC-SSM is an integrated service member to the Cisco ASA platform. All other capabilities can be used in parallel with the CSC-SSM to provide maximum protection, control, and secure communications.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C67-328546-03 8/07