Cisco ASA 5500 Series Content Security and Control Security Services Module and the Children's Internet Protection Act

The Cisco® ASA 5500 Series Content Security and Control Security Services Module (CSC-SSM) delivers industry-leading threat protection and content control at the Internet edge. The CSC-SSM provides comprehensive antivirus, antispyware, file blocking, antispam, antiphishing, URL blocking and filtering, and content filtering services in a comprehensive, easy-to-manage solution.

The CSC-SSM bolsters the Cisco ASA 5500 Series' strong security capabilities, providing customers with additional protection and control over the content of their Internet communications. It scans email, web traffic, and files transferred from the Internet to protect the network against threats such as spam, spyware, and viruses. It is optimized for small and medium-sized organizations and remote branches through its simplified deployment and ease of use.

The CSC-SSM is ideally suited to help U.S. public schools and libraries adhere to the requirements of the Children's Internet Protection Act (CIPA), a federal law that was enacted by the U.S. Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers.[1] CIPA imposes certain types of requirements on schools or libraries that receive funding support for Internet access or internal connections from the E-rate program, which makes certain types of technology more affordable for eligible schools and libraries.

In early 2001, the Federal Communications Commission (FCC) issued rules for the implementation of CIPA.

1. An Internet safety policy must include technology protection measures to block or filter Internet access on computers that are accessed by minors for pictures that: (a) are obscene, (b) are child pornography, or (c) are harmful to minors.
2. Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors.
3. Schools and libraries subject to CIPA are required to adopt and implement a policy addressing the following: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) the restriction of minors' access to materials harmful to them.[2]

The Cisco CSC-SSM product can provide a full featured set of protections consistent with the requirements of CIPA. Table 1 outlines the salient features of the CSC-SSM.

[1] Federal Communications Commission Website, July 2007.
[2] CIPA Section 1732: Internet Safety Policy Required (http://ifea.net/cipa.html).

Table 1. CIPA Requirements Enabled by the Cisco CSC-SSM

Safety Requirement	Feature Support for Requirement	Coverage
Include technology protection measures to block or filter Internet access to pictures that are obscene, are child pornography, or are harmful to minors, for computers that are accessed by minors	Content filtering database of millions of URLs broken into categories, including “pornography”, “nudity”, and “violence/hate crime”	Yes
	URL whitelisting and blacklisting options (“allowed” and “not-allowed”)	Yes
Adopt and enforce a policy to monitor online activities of minors	Monitoring and reporting tools for blocked sites	Yes
Prevent access by minors to inappropriate matter on the Internet	Content filtering database of millions of URLs broken into categories, including “pornography”, “nudity”, and “violence/hate crime”	Yes
	URL whitelisting and blacklisting options (“allowed” and “not-allowed”)	Yes
Address the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications	Antispam, antiphishing, and content filtering for email traffic	Yes
	File type blocking	Yes
	URL whitelisting and blacklisting options (“allowed” and “not-allowed”)	Yes
Prevent unauthorized access, including “hacking” and other unlawful activities by minors online	Prevents downloading of keylogger and identity theft	Yes
	Automated cleanup of spyware and malware infections	Yes*
	Prevents new spyware infections	Yes
	Blocks hacked, hijacked, or otherwise compromised systems, both internally and externally	Yes
Prevent unauthorized disclosure, use, and dissemination of personal identification information regarding minors	Prevents downloading of keylogger and identity theft	Yes
	Antispam, antiphishing, and content filtering of email traffic	Yes
	Prevents new spyware infections	Yes
	Automated cleanup of spyware and malware infections	Yes*
Address measures designed to restrict minors' access to materials that are harmful to minors	Content filtering database of millions of URLs broken into categories including “pornography”, “nudity”, and “violence/hate crime”	Yes
	URL whitelisting and blacklisting options (“allowed” and “not-allowed”)	Yes

* Feature enabled through integration with Trend Micro Damage Cleanup Services (provided separately).

While Cisco cannot guarantee complete compliance with CIPA, Table 1 summarizes the areas where the Cisco ASA 5500 Series CSC-SSM provides technology solutions in support of the act’s provisions. Schools and libraries should perform their own evaluation of how the CSC-SSM would apply to their environment.

For More Information

For more information about the Cisco ASA 5500 Series CSC-SSM, visit http://www.cisco.com/en/US/products/ps6120/index.html.

For more information about CIPA, visit http://www.fcc.gov/cgb/consumerfacts/cipa.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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 C11-483382-00 06/08