CIPA Compliance and the Barracuda Spyware Firewall

RELEASE 1
MAY 2006

History

The Children's Internet Protection Act (CIPA) was enacted by Congress in December 2000 and requires schools and libraries to certify that they have an Internet Safety Policy in place in order to qualify for the "E-Rate" program – a program designed to make technology more affordable to eligible schools and libraries. After being signed into law, the Federal Communications Commission (FCC) issued the following guidelines on implementing CIPA, which became effective in April 2001:

What CIPA Requires

1. Schools and libraries subject to CIPA may not receive the discounts offered by the E-Rate program unless they certify that they have an Internet safety policy and technology protection measures in place. An Internet safety policy must include technology protection measures to block or filter Internet access to pictures that: (a) are obscene, (b) are child pornography, or (c) are harmful to minors, for computers that are accessed by minors.

2. Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors; and

3. Schools and libraries subject to CIPA are required to adopt and implement a policy addressing: (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) restricting minors' access to materials harmful to them.

Schools and libraries are required to certify that they have their safety policies and technology in place before receiving E-Rate funding.

Source: Federal Communications Commission: "Children's Internet Protection Act"
http://www.fcc.gov/cgb/consumerfacts/cipa.html

Content Filtering and CIPA Compliance

The CIPA rules state that schools and library computers must demonstrate that they have a solution in place to address the rules put forth by the FCC. In order to ensure they are able to "monitor the online activities of minors" and have policies addressing the safety of minors by blocking or filtering access to obscene, pornographic, or harmful communications. A solution must be put in place to monitor and limit Web access to prohibited sites.

In addition to protecting the overall security of a computer network, the Barracuda Spyware Firewall also provides the specific content filtering protections typically required to enforce policies necessary to obtain CIPA compliance.

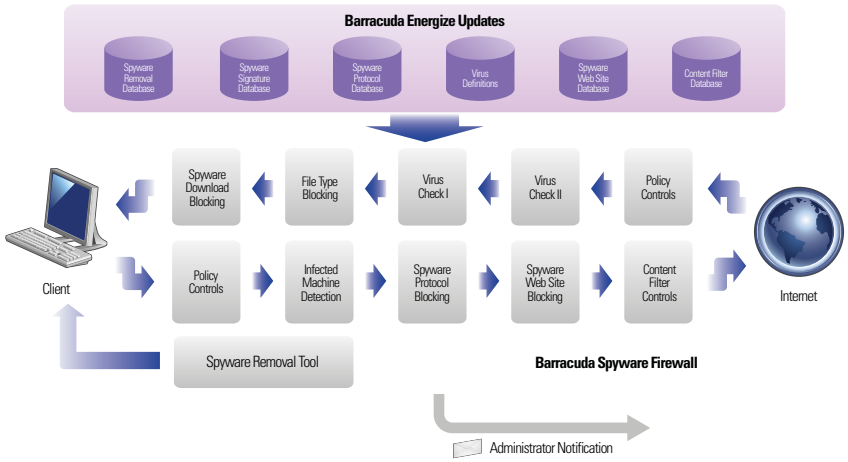
The Barracuda Spyware Firewall

Content filtering has always been an important strategy for blocking spyware. In addition to hosting controversial content, pornography, violence, and other "fringe" sites have long been hosts to spyware and other malware threats. To block access to these sites, the Barracuda Spyware Firewall includes a pre-installed URL list containing millions of URLs classified into 57 categories for easy and efficient content filtering. This list is continuously updated by engineers at Barracuda Central and delivered hourly via the Energize Updates subscription service sold with the Barracuda Spyware Firewall.

Schools and libraries seeking CIPA compliance prefer the Barracuda Spyware Firewall because of the simplicity of its use and design. Unlike competing Web content filtering solutions, the Barracuda Spyware Firewall was originally designed to provide universal security protection to computer networks, rather than as a means to control policies at an extreme level of granularity. As such, typical installations take hours, not days, and the Barracuda Spyware Firewall is priced far more attractively compared to competing solutions.

In developing content filtering policy for the Barracuda Spyware Firewall, Barracuda Central, an advanced technology operations center where engineers constantly monitor the Internet for trends in spam, virus and spyware threats, has leveraged both Web crawling technologies and its network of spam honeypots and customer opt-in systems to monitor those sites most heavily promoted and visited on the Internet. Unlike competing solutions which simply build large URL databases independent of popularity, Barracuda Networks is effective at blocking those sites that currently receive 99 percent of the Internet traffic in their respective categories.

Barracuda Spyware Firewall Architecture



Award-Winning Content Filtering & Spyware Prevention

Content filtering is central to providing CIPA compliance. The Barracuda Spyware Firewall provides 57 content categories including:

- Destructive sites such as those promoting violence, illegal drugs, or criminal activity
- Sexual sites that may contain adult material or pornographic content
- Gaming/gambling
- Leisure sites (i.e. tobacco and alcohol)

Specific sites can also be blocked or allowed using explicit block and allow lists, and downloads can be limited to only specific approved file types. The Barracuda Spyware Firewall provides additional cutting edge tools like URL rewriting, which can automatically enforce safe search tags for sites like Google images and video, preventing children from circumventing protection policies through the media caches of popular search engines.

In addition to blocking content, the Barracuda Spyware Firewall protects other malware threats, such as unauthorized key-logging and personal information theft. These activities are unlawful and can be extremely dangerous to minors as well as institutions and corporations. The Barracuda Spyware Firewall is extremely effective at blocking and reporting such malicious activity. It not only stops the transport of the stolen information, it also includes the Barracuda Spyware Firewall Removal Tool, a utility to clean the infected machines.

Application Blocking and Client Lockdown

The Barracuda Spyware Firewall enables administrators to easily select Internet applications to block or allow. For example, a single checkbox can block Instant Messaging (IM) traffic and eliminate a frequently used criminal channel for soliciting minors.

The Client Lockdown feature enables administrators to disable Internet access from systems that have been hacked, hijacked, or otherwise compromised.

Barracuda Networks Enables CIPA Compliance

The Barracuda Spyware Firewall is ideally suited to help public schools and libraries enforce CIPA policies in an easy and cost effective manner. Used in combination with the Barracuda Spam Firewall to manage email use, and the Barracuda IM Firewall for managing IM traffic, Barracuda Networks' products can enable CIPA compliance for nearly all facets of a network.

The Barracuda Spyware Firewall enables CIPA compliance with the following protections:

CIPA Requirement*	Barracuda Networks Technology
1(a)(b)(c), 3(a)(c)(e)	Content filtering database of millions of URLs broken into 57 categories for targeted content filter policies.
1(a)(b)(c), 3(a)(e)	Safe Search features to block the media caches of popular search engines
2	Identification of where threats are coming from, both externally and internally
1(a)(b)(c), 3(a)(c)(e)	URL block and allow lists
1(c), 2, 3(a)(c)(e)	File type blocking
3(c)(d)	Prevention of keystroke logging and personal information theft
1(a)(b)(c), 3(a)(d)(e)	Monitoring of Web traffic for virus and spyware downloads
1(a)(b)(c), 3(a)(d)(e)	Inspection of network traffic for spyware infection activity
3(b)	Instant Message blocking
3(c)(e)	Client Lockdown features to prevent system hacking and hijacking
3(c)(e)	Examination of inbound and outbound spyware and Web surfing activity
3(c)(e)	Prevention of new spyware infections
3(c)(e)	Clean up of detected infections from Windows desktop computers through the Barracuda Spyware Removal Tool
1(a)(b)(c), 3(a)(e)	Blocking applications which can be dangerous to the minors
3(c)(e)	Blocking hacked, hijacked, or otherwise compromised systems

**corresponds to the numbers/sections in the "What CIPA Requires" section of this document*

Location, Location, Location

Since the Barracuda Spyware Firewall sits inline on your network, all traffic passes through it. This gives the product the ability to intercept, manage, and redirect, not only spyware and malware, but curious young Web surfers.

Typical Deployment

Powerful, Easy, and Affordable

Barracuda Networks has become a leading provider of Spyware, Email, and IM security solutions by providing our customers with powerful products with the options they require and which can be easily installed and maintained at a price that they can afford. Join the more than 35,000 customers worldwide who put their trust in Barracuda Networks.

CIPA compliance is a complex problem with an easy solution: The Barracuda Spyware Firewall.

About Barracuda Networks, Inc.

Barracuda Networks is the leading provider of enterprise-class application security appliances for comprehensive email, Internet and IM protection. Its products protect over 35,000 customers around the world, including Adaptec, Caltrans, CBS, Georgia Institute of Technology, IBM, Knight Ridder, NASA, Pizza Hut, Union Pacific Railroad Company, and the U.S. Treasury Department. The Barracuda Spam Firewall and Barracuda Spam Firewall - Outbound protect organizations against spam, viruses, and violations to e-mail security policy. The Barracuda Spyware Firewall offers comprehensive content filtering and complete network protection against spyware, malware and viruses. The Barracuda IM Firewall, is the only all in one gateway solution for IM traffic management and security. Barracuda Networks is a privately held company with headquarters in Mountain View, California. Barracuda Networks has offices in eight international locations and distributors in over 43 countries.
More information is available at www.barracudanetworks.com.

Barracuda Networks
385 Ravendale Drive
Mountain View, CA 94043
United States
+1 408.342.5400
www.barracudanetworks.com
info@barracudanetworks.com