CIPA Compliance and the Barracuda Web Security Gateway

White Paper

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding support for Internet access or internal connections from the "E-Rate" program – a program that makes certain technology more affordable for eligible schools and libraries. In early 2001, the Federal Communications Commission (FCC) issued rules implementing CIPA.

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 that includes technology protection measures. 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 must provide for educating minors about appropriate online behavior.
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.

*Please refer to the CIPA Requirements chart on page 3 for more information

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 Web Security Gateway also provides the specific content filtering protections typically required to enforce policies necessary to obtain CIPA compliance.

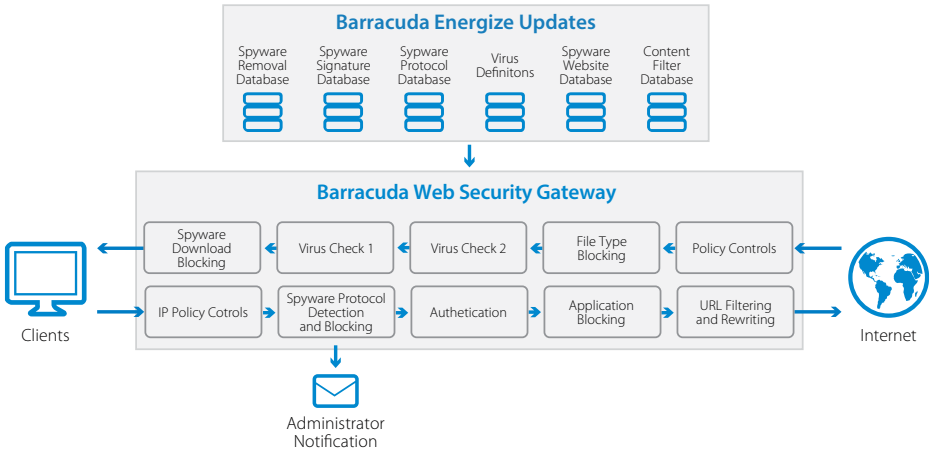
The Barracuda Web Security Gateway

Content filtering is becoming increasingly important in most organizations. Controlling access to controversial and offensive content such as pornography, violence, hacking, and other "fringe" sites has become a necessity. To block access to these sites, the Barracuda Web Security Gateway includes a preinstalled URL list containing millions of URLs classified into 95 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 Web Security Gateway.

In developing content filtering policy for the Barracuda Web Security Gateway, Barracuda Central 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.

Schools and libraries seeking CIPA compliance prefer the Barracuda Web Security Gateway because of the simplicity of its use and design. Typical installations take hours, not days, and the Barracuda Web Security Gateway is far more attractively priced compared to competing solutions. As an added value, the Barracuda Web Security Gateway also provides award-winning protection against spyware and other malware threats by blocking downloads of malicious content and scrubbing infected machines.

Barracuda Web Security Gateway Architecture



Award-Winning Content Filtering & Spyware Prevention

Content filtering is central to providing CIPA compliance. The Barracuda Web Security Gateway provides 95 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 sites
- 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 Web Security Gateway 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 Web Security Gateway protects other malware threats, such as unauthorized keylogging and personal information theft. These activities are unlawful and can be extremely dangerous to minors and institutions and corporations. The Barracuda Web Security Gateway is extremely effective at blocking and reporting such malicious activity. It not only stops the transport of the stolen information.

Application Blocking and Client Lockdown

The Barracuda Web Security Gateway 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

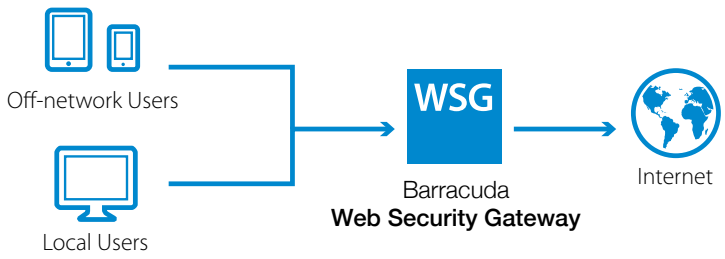
The Barracuda Web Security Gateway is ideally suited to help public schools and libraries enforce CIPA policies in an easy and cost effective manner. When used in combination with the Barracuda Email Security Gateway to manage email use, Barracuda Networks' products can enable CIPA compliance for nearly all facets of a network.

CIPA REQUIREMENT*	BARRACUDA NETWORKS TECHNOLOGY
1(a)(b)(c), 3(a)(c)(e)	Content filtering database of millions of URLs broken into 95 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

Location, Location, Location

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

Powerful, Easy, and Affordable



Barracuda Networks is the trusted source for spam, spyware, virus, and content blocking. Organizations seeking powerful products with the options they require, that can be easily installed and maintained at an affordable price, choose Barracuda. Join the more than 150,000 customers worldwide who put their trust in our products.

CIPA compliance is a complex problem with an easy solution: the Barracuda Web Security Gateway

For questions about the Barracuda Web Security Gateway, please visit http://www.barracuda.com/webfilter or call Barracuda Networks for a free 30-day evaluation at +1 408-342-5400. For more information on our other security and productivity solutions, please visit http://www.barracuda.com/products.

About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud, and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com