Barracuda
Your journey, secured.

CIPA compliance with Barracuda SecureEdge SASE Platform and Barracuda CloudGen Firewall

WHITE PAPER

NETWORK SECURITY

Introduction

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 internet 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. A high-level overview of the current CIPA regulations can be found here. The full act is available as CHILDREN'S INTERNET PROTECTION ACT (Pub. L. 106-554) on the e-rate website. An analysis prepared for the American Library Association with further details is available on the American Library Association website.

Content filtering and CIPA compliance

Content filtering is becoming increasingly important in most organizations. Controlling access to controversial and offensive content such as pornography, violence, hacking, etc., has become a necessity.

To block access to these sites, every Barracuda SecureEdge site device includes full Secure Web Gateway functions including web filtering with content classification in 201 categories that are again classified in 19 super-categories for easy and efficient management. This list is continuously updated by engineers at Barracuda Central and delivered continuously via the basic Energize Updates subscription.

SecureEdge site devices use the same content filtering engine and employ the same easy to use web-based management principles as the Barracuda Web Security Gateway that tens of thousands of school districts in the around the world trust because of the simplicity of its use. Typical installations take hours, not days, and Barracuda SecureEdge site devices provide better performance, deliver more functionality, and are more attractively priced compared to competing solutions.

Additionally, every SecureEdge site device provides full control for thousands of applications, including anti-malware with cloud-based Advanced Threat Protection and sandboxing, provides Web monitoring, and safe search. SecureEdge can easily be used to provide ZTNA access, network segmentation and Secure Internet Access for Work-from-Anywhere (WFA) scenarios should the needs arise.

What CIPA requires

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.

The protection measures must block or filter Internet access to pictures that are:

(a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors).

Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements:

1) their Internet safety policies must include monitoring the online activities of minors; and

2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them.

Schools and libraries must certify they are in compliance with CIPA before they can receive E-rate funding.

Source: https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

CIPA requirement	Barracuda SecureEdge and Barracuda CloudGen Firewall
The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors.	User and group-dependent security policies, application control, URL filtering, and SafeSearch enforcement, even for TLS/SSL encrypted websites, provided by every Barracuda SecureEdge site device and Barracuda CloudGen Firewall appliance with an active Energize Updates subscription.
Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors	Barracuda SecureEdge and Barracuda CloudGen Firewall include monitoring of web content including keyword search to find potentially harmful uploads and search terms.
Schools subject to CIPA have two additional certification requirements: 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response	URL filter capability with Barracuda SecureEdge and Barracuda CloudGen Firewall provides click-and-proceed block pages that are used to provide guidance for use of online resources like social networking websites, chat rooms, and others.
Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: • Access by minors to inappropriate matter on the Internet;	Barracuda SecureEdge and Barracuda CloudGen Firewall provide user and group-dependent security policies, application control, URL filtering, and SafeSearch enforcement, even for TLS/SSL encrypted websites with an active Energize Updates subscription: 201 web filter categories classified in 19 super categories and an easy-to-implement user interface enable quick deployment.
Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: • The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;	Barracuda SecureEdge and Barracuda CloudGen Firewall provide user and group dependent security policies, application control, URL filtering, and SafeSearch enforcement, even for TLS/SSL encrypted websites with an active Energize Updates subscription. Instant messaging or other unsanctioned apps can be blocked for individual users or user groups. For many other applications, the use can be sanctioned to, e.g., read-only. Web monitoring with built-in keyword filters for adultery/porn, cyberbullying, weapons/violence, and terrorism as well as custom keyword filters helps keeping minors safe.
Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: • Unauthorized access, including so-called “hacking,” and other unlawful activities by minors online;	Barracuda SecureEdge and Barracuda CloudGen Firewall include full next-generation firewall technology, intrusion prevention, and IP-rate limiting to enable network segmentation and prevent from hacking attempts or DDoS attacks.
Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: • Unauthorized disclosure, use, and dissemination of personal information regarding minors;	Barracuda SecureEdge and Barracuda CloudGen Firewall include keyword filters, file type filters, and basic proxy-based CASB functionality.
Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: • Measures restricting minors’ access to materials harmful to them.	Barracuda SecureEdge and Barracuda CloudGen Firewall include URL filtering, malware protection with Barracuda Advanced Threat Protection, IPS, and application control including the ability for custom categories and block/allow lists. This prevents access to applications and websites that can be dangerous to minors.

Barracuda
Your journey, secured.

More than 200,000 global customers trust Barracuda to safeguard their employees, data, and applications from a wide range of threats. Barracuda provides easy, comprehensive and affordable solutions for email protection, application protection, network protection and data protection. We are continually innovating to deliver tomorrow's security technology, today.

For more information about other Barracuda successes, please visit: blog.barracuda.com

Barracuda CloudGen Firewall™

Barracuda CloudGen Firewall provides a comprehensive set of next-generation firewall technologies to ensure real-time network protection against a broad range of network threats, vulnerabilities, and exploits, including SQL injections, cross-site scripting, denial of service attacks, trojans, viruses, worms, spyware, and many more. Secure SD-WAN functionality integrated in Barracuda CloudGen Firewall lets you ensure that there is always enough bandwidth for business-critical applications.

Barracuda SecureEdge™

Barracuda SecureEdge secures your users, sites and things with an easy-to-deploy cloud-first platform that connects any device, application and cloud/hybrid environment.

SecureEdge provides zero-trust application access to any type of application, cloud-based security for endpoints, and automated SD-WAN connectivity for sites and industrial facilities of any type and size.

Barracuda
Your journey, secured.