Barracuda
Your journey, secured.

How Schools and Libraries Can Get CIPA Compliance Help

Meeting federal E-Rate requirements is quick and easy with Barracuda's CloudGen Firewall.

NETWORK SECURITY

How Schools and Libraries Can Get CIPA Compliance Help

Meeting federal E-Rate requirements is quick and easy with Barracuda's CloudGen Firewall.

Summary

- Compliance with the Children's Internet Protection Act (CIPA) is mandatory for any school or library seeking federal funding.
- Barracuda CloudGen Firewall is an easy, affordable, and top-rated product for help in certifying CIPA requirements.
- Additionally, CloudGen Firewall provides best-in-class cybersecurity to keep your organization and users safe from costly digital attacks and fraud.

Introduction

At the turn of the century, Congress passed the Children's Internet Protection Act (CIPA) into United States law. Five years after the world wide web went mainstream, the legislation was enacted to address and restrict access to offensive content over the Internet from school and library computers. Now regulated by the Federal Communications Commission (FCC), CIPA imposes certain requirements on any school or library that receives federal funding or subsidies, such as the popular E-Rate program, which provides discounted internet access to qualifying schools and libraries. Here's what interested parties need to know.

Understanding requirements

According to CIPA, schools and libraries may not receive discounts offered by E-Rate or any other public-funding programs unless they certify and enforce an Internet Safety Policy (ISP) with the appropriate technology measures. In short, CIPA demands that said ISPs must block or filter all access to pictures that are obscene, pornographic, or harmful to minors.

On top of that, schools are subject to two additional certification requirements: 1) their Internet safety policies must monitor and log the online activity of minors; and 2) as required by the Protecting Children in the 21st Century Act, schools must instruct minors about appropriate online behavior, including interacting with other individuals over email, on social networking websites, in chat rooms, and cyberbullying awareness and response.

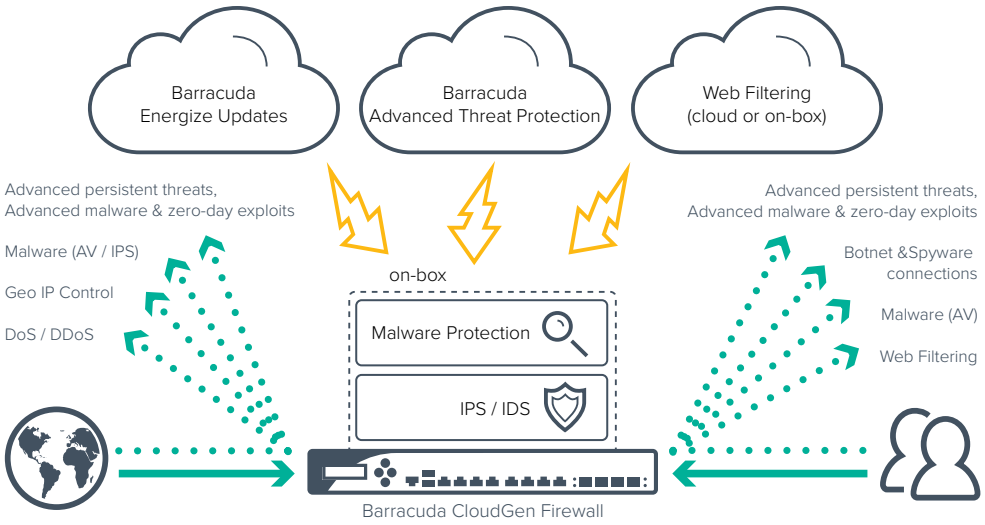
Additionally, ISPs must use technology measures to prevent unauthorized access (or so-called "hacking") and other unlawful activities by minors online, including unauthorized disclosure, use, and dissemination of personal information regarding minors, and restricting minors' access to any other materials deemed harmful to them.

In short, CIPA demands a lot from school and library administrators, in addition to any technology they choose to help certify and enforce the law. Before receiving any government funding, said technology must restrict and monitor online activity, block or filter inappropriate images from Internet-connected computers, and (for schools) provide reasonable public notice and education on internet safety.

CIPA demands a lot from school and library administrators, in addition to any technology they choose to help certify and enforce the law.

A compelling response

With an online user review rating of nearly five perfect stars, Barracuda CloudGen Firewall is the ideal way for schools and libraries to enforce CIPA policies both quickly and affordably. When used in combination with the Barracuda Email Security Gateway, Barracuda Networks can help with CIPA compliance in nearly all facets of your organization.



Barracuda CloudGen Firewall's web security architecture

With an online user review rating of nearly five perfect stars, Barracuda CloudGen Firewall is the ideal way for schools and libraries to enforce CIPA policies both quickly and affordably.

With over 150,000 customers worldwide, including countless schools and libraries, Barracuda Networks is one of the most trusted tools for CIPA compliance help, E-Rate discounts, and even more importantly, cyber security against spam, spyware, virus, and undesired or otherwise inappropriate content. Thanks to its reputation for both ease of installation and affordability, Barracuda Networks makes an often complex and daunting process seem easy, if not push-button.

In short, CloudGen Firewall is a family of physical (on-premises), virtual, and cloud-based appliances that protect and enhance your expanding network infrastructure. This leading firewall includes a comprehensive set of next-generation technologies, including Layer 7 application profiling, intrusion prevention, web filtering, advanced malware protection, antispam protection, and network access control.

Additionally, CloudGen Firewalls combine highly resilient VPN technology with intelligent traffic management and WAN optimization capabilities. This lets you reduce line costs, increase overall network availability, improve site-to-site connectivity, and ensure uninterrupted access to applications (and CIPA compliance support) hosted in the cloud. And centralized management helps you reduce administrative overhead while defining and enforcing granular policies across your entire network.

Exceeding compliance

Although CIPA compliance is a critical factor for schools and libraries seeking E-Rate or other federal subsidies, there are other protective tasks schools and libraries must fulfil that are neither required nor regulated—cybersecurity is chief among them. After nearly two decades of experience, Barracuda Networks put all of that know-how into its latest CloudGen Firewall to not only satisfy CIPA requirements, but to protect your organization both on-premises and in the cloud.

Although CIPA compliance is a critical factor for schools and libraries seeking E-Rate or other federal subsidies, there are other protective tasks schools and libraries must fulfil that are neither required nor regulated—cybersecurity is chief among them.

In the multi-device era, network firewalls must do more than just secure your network. They must also ensure you have uninterrupted network availability and access to cloud-hosted applications, such as Google apps, Dropbox, Adobe Creative

Cloud, and popular social media platforms. In addition to schools and libraries, CloudGen Firewalls are ideal for multi-site organizations, managed service providers, and anyone else with complex or otherwise dispersed networks.

Why? Cloud protection against advanced threats and zero-hour attacks is a big deal. So is affordable cybersecurity, secure SD-WAN, anytime application access, remote access for off-network users, interoperability between public and hybrid cloud environments, and best-in-class network controls and monitoring.

What's included

In addition to CIPA compliance support and best-in-class cybersecurity, CloudGen Firewall offers both a breadth and depth of features. Namely:

- Advanced threat protection. CloudGen Firewall uses Barracuda's next-generation sandbox technology to catch persistent threats, zero-day malware, and all other hacks designed to evade detection. This is achieved through multiple datacenters in the Americas, mainland Europe, and the UK and tens of thousands of continuously updated CloudGen Firewalls, Email Security Gateways, Web Security Gateways, and Barracuda Essentials.
- Customizable, on-demand analysis reports. To keep you informed, CloudGen Firewall provides full insight and details on malicious activities, file behavior, system-registry entries, and evasion and obfuscation techniques. This also enables network activities such as establishing encrypted connections to botnet commands and control centers for increased security posture to evade further attack.
- Botnet and spyware protection. In combination with advanced threat protection, all Barracuda CloudGen Firewalls detect and protect against botnet infections and DNS requests. Once an infected client is detected, it can be isolated automatically, and an alert can be created or reported with the Barracuda Firewall Report Creator.
- TypoSquatting and email link protection. This important feature of advanced threat protection adds protection for two rising threats: uncovering misleading and misspelled links. The link protection component automatically rewrites deceptive URLs in email messages to a Barracuda-validated URL and informs the requesting user of this change via a warning page so you stay protected.
- Web filtering. This comes standard with the Energize Updates subscription and enables highly granular, real-time visibility into online activity—broken down by individual users and applications—thereby letting administrators create and enforce effective Internet content and access policies. Web filter functionality with Barracuda CloudGen Firewalls protects user productivity, blocks malware downloads and other web-based threats, helps you meet compliance standards by blocking access to inappropriate websites and servers, and provides an additional layer of security alongside your network control.
- Safe search enforcement. Many search engines have a safe search setting to filter out adult results such as inappropriate images and videos. On Barracuda CloudGen Firewalls customers can easily activate Safe Search Enforcement so that the firewall will enforce safe search settings for all common search providers such as Google, Yahoo, and Bing, and even within YouTube. Unsupported search engines can then be easily blocked.
- Google accounts enforcement. In some cases, users with their own Google Apps account may be able to circumvent Safe Search enforcement settings by logging in from their workstation with their own Google Apps account. To prevent this, all Barracuda CloudGen Firewalls enforce and limit Google Apps logins to predefined Apps accounts that were previously created by the administrator.
- Mail security gateway. Mail is still one of the most common ways of spreading malware. Thankfully, CloudGen Firewalls include all the necessary means to prevent incoming email from infecting corporate mail servers. CloudGen Firewall mail security includes malware scanning, advanced threat protection, and basic spam filtering via DNS block-listing of known mail senders and malware domains.
- Malware protection. The optional Malware protection shields internal networks by scanning web content (HTTP and HTTPs), email (SMTP, POP3), and file transfers (FTP) via two fully integrated antivirus engines. Malware protection is based on regular signature updates as well as heuristics to detect malware or other potentially unwanted programs—even before signatures are available.
- File content enforcement. CloudGen Firewall includes true file type detection and enforcement capabilities based not only on extension and MIME type, but also on sophisticated true file type detection algorithms. Bypassing executable files by renaming or compressing is detected and blocked. Besides blocking and allowing connections, CloudGen Firewall also lets admins change download priorities. For example, if an ISO image started downloading with normal web traffic priority, the

admin can increase or decrease the assigned bandwidth for the download, even though the user started downloading via a regular web-browsing session.

- Award-winning content filtering and spyware prevention. Content filtering is central in meeting CIPA compliance. Fortunately, CloudGen Firewall's web filtering capabilities offer 95 content categories to more than 200 million categorized URLs covering 90 percent of the top one million websites. In addition to autodetection of destructive websites, specific sites can also be blocked or allowed.
- Keylogging and personal threat protection. In addition to blocking content, CloudGen Firewall protects other malware threats, such as unauthorized keylogging and personal information theft. These activities are unlawful and can be extremely dangerous to minors, institutions, and corporations. Barracuda CloudGen Firewall is extremely effective at blocking and reporting such malicious activity.
- Application blocking and quarantine. What's more, CloudGen Firewall allows administrators to easily allow or block select internet applications and traffic. For example, you can block Instant Messaging (IM) traffic and/or eliminate a frequently used criminal channel for soliciting minors. Or just blocking downloads or certain sub- protocols of applications (e.g., Facebook Games) during teaching hours.
- Constant protection. Since Barracuda CloudGen Firewall is the core of network security, 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.

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 (quarantine) 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

Learn more

To further determine if CloudGen Firewall and other Barracuda products are right for your school, library, or similar organization, please visit Barracuda CloudGen Firewall, call 1 (844) 543-2053 with any questions, or contact us online.

Barracuda®
Your journey, secured.