Meeting CIPA compliance with Fortinet

CIPA Requirements

Federal law HR4577, better known as the Children's Internet Protection Act (CIPA), was enacted by Congress in December of 2000. The Federal Communications Commission (FCC) then issued rules to ensure enforcement of CIPA requirements. In order to receive E-Rate discounts for Internet access and internal connection services under the Universal Service Fund (USF), CIPA requires certain K-12 schools and library authorities to certify that they are enforcing a policy of Internet safety.

Schools and libraries subject to CIPA are required to adopt a policy that addresses

(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. Security measures must be able to block or filter pictures that are obscene or contain child pornography for both minors and adults.

Fortinet Solution

Fortinet offers products that can help you achieve CIPA compliance, ensuring E-Rate discounts for your school or library. FortiGate® multi-threat security appliances integrate purpose-built hardware and software to monitor your network and filter Internet traffic for inappropriate content in real time.

Unwanted Internet-based applications, such as Facebook, Twitter and Skype can be fully blocked or only partially enabled as needed, on an individual or group basis. Antivirus, IPS and DLP (Data Leak Prevention) can add additional protection against malicious content, unlawful activities and unauthorized disclosure.

FortiGuard® Services provide regular updates to Web Filtering and Antivirus protections, blocking student access to undesirable Web sites and removing the latest threats before they can infect endpoints. For large campuses and installations, FortiManager™ and FortiAnalyzer™ appliances enable single pane-of-glass management with extensive logging and archiving capabilities to enhance oversight and simplify auditing centrally with distributed FortiGates.

Learn More

Visit Fortinet at http://www.fortinet.com/solutions/education.html or call 866-868-3678. Fortinet solutions will help you achieve CIPA compliance while protecting students and faculty from exposure to inappropriate content.

The table below summarizes the areas where FortiGate provides technology solutions in support of the act's provisions.

CIPA Requirement	Security Feature Support on FortiGate
Prevent access to minors to inappropriate matter on the Internet	Web Filtering – Blocks sites under inappropriate categories such as adult/ mature content
	Manual Website Blacklisting – Blocks webpages by keywords or URLs.
	Safe Search Enforcement –Rewrites search queries with Safe Search options to deliver child appropriate results.
Address the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications	Antivirus – Detects malicious attachments or file transfers over electronic communications
	Anti-spam, DLP – Filters malicious or inappropriate content
	Web Filtering –Restrict social media and online communication sites if necessary
Prevent unauthorized access, including "hacking" and other unlawful activities by minors online	Firewall –Enforces access to other networks and Internet. Users Authentication can also be implemented.
	Application Control – Prevents usage of malicious applications
	IPS –Detects and blocks unlawful activities, terminal can be quarantined till further investigation
Prevent unauthorized disclosure, use, and dissemination of personal identification information regarding minors	Firewall – Prevents unauthorized access to internal hosts
	Antivirus –Mitigates malicious code infections which allows external controls
	DLP – Protects against servers and terminals from disclosing personal information
Address measures designed to restrict minors' access to materials that are harmful to minors	Web Filtering –Blocks sites under inappropriate categories such as violent content
	Manual Website Blacklisting – Blocks webpages by keywords or URLs
	Safe Search Enforcement –Rewrites search queries with Safe Search option to deliver child appropriate results

SG-CIPA-201202