EXCEED CIPA COMPLIANCE WITH PALO ALTO NETWORKS

The Children's Internet Protection Act[1] is a federal law enacted by the United States Congress to address concerns around internet access in K-12 schools and libraries. To receive E-rate federal funding, schools and libraries must meet CIPA requirements.

Palo Alto Networks, the world's cybersecurity leader, enables schools to maximize student and data protection with minimal network and security resources. Palo Alto Networks Next-Generation Firewalls natively integrate multiple innovations and automation into one platform, eliminating security point products while simplifying security management and compliance. Schools rely on Palo Alto Networks to:

- Keep students safe from the latest inappropriate content and malicious sites with realtime intelligence and automated protection.
- Easily create and enforce flexible security policies for different users, applications, devices, and data.
- Simplify security management by monitoring minors' activity along with security policies, threats, and logs through a single pane of glass.
- Consistently protect data center, school, mobile, and cloud environments.
- Protect the latest digital innovations without adding more appliances or user interfaces.

Keep Students and Data Safe with a Platform Approach to Cybersecurity

Our Next-Generation Firewalls eliminate the need to buy, deploy, integrate, and separately manage multiple point products, reducing the cost and complexity of cybersecurity. Schools can choose to leverage some or all security technologies supported by standalone or virtualized firewalls to protect schools, data centers, and cloud environments. While Next-Generation Firewall features and subscriptions protect students and school operations and data in myriad ways, the table that follows provides an overview of how its capabilities contribute to CIPA compliance.

Minimum Compliance Requirements: Filtering, Visibility, and Control

Schools can meet CIPA requirements as well as keep their students, data, and operations safe with Palo Alto Networks Next-Generation Firewalls and tightly integrated innovations. At a minimum, schools should implement:

- **URL Filtering:** This subscription for Next-Generation Firewalls hosts information about hundreds of millions of websites and more than 75 URL categories, including Adult, Abused Drugs, Hacking, and other categories relevant to CIPA. URL Filtering also categorizes URLs by risk level, accounting for factors like time since registration and whether URLs are hosted on dynamic DNS platforms. URL Filtering allows schools to:
    - Block access to high-risk or inappropriate website categories.
    - Enforce Safe Search.
    - Enforce restricted YouTube access.
    - Create alerts and perform actions based on keyword searches in search results.
    - Prevent inappropriate content from appearing in minors' search results.
    - Thwart common evasion tactics, such as cached results and language translation sites.

[1] Federal Communications Commission Children's Internet Protection Act, https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.

Palo Alto Networks Next-Generation Firewall Capabilities That Contribute to CIPA Compliance Across Endpoint, Network, and Cloud Environments

CIPA Requirement	Minimum Requirements for CIPA Compliance					Best Practices to Reduce Risk					
	URL Filtering*	User Identification	Application Identification	SSL Decryption	Threat Prevention*	Zero-Day Malware Prevention	Remote Security*	Data Filtering Profiles	Zero Trust Network Segmentation	Credential Theft Prevention	DNS Security*
Web filtering to block images that are obscene, contain child pornography, or are harmful to minors	✓	✓	✓	✓		✓	✓				
Online activity monitoring of minors	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Prevention of access by minors to inappropriate material on the internet	✓	✓	✓	✓			✓	✓			
Assurance of minors' safety when using email, chat rooms, etc.	✓	✓	✓	✓			✓				
Blocking of unauthorized access, hacking, and other unlawful activities by minors online	✓	✓	✓	✓	✓		✓	✓		✓	✓
Prevention of disclosure, dissemination, or use of minors' personal information		✓	✓	✓	✓			✓		✓	✓
Restricted access to materials harmful to minors	✓	✓	✓	✓	✓			✓		✓	✓

*Capability available by subscription

- **User identification (User-ID™ technology):** This standard feature on every Next-Generation Firewall enables schools to create and view policies, reporting, and forensics based on users and groups—not IP addresses. Administrators can associate students with their network activity, gaining insight that can meet monitoring requirements, help refine security and network usage policies, and reduce incident response times. Next-Generation Firewalls leverage user information from a wide range of repositories, including LDAP services such as Microsoft Active Directory®, Microsoft Exchange, and Novell eDirectory; XML APIs; and syslog messages from wireless LAN controllers and other devices.
- **Application identification (App-ID™ technology):** This patented technology identifies and controls more than 3,000 applications, irrespective of port, protocol, SSL encryption, or evasive tactics. Schools can foster education and research while controlling access to applications and content harmful to minors. Working in conjunction with URL Filtering and User-ID, App-ID enables schools and districts to:
    - Allow, deny, or even bandwidth-limit applications for an entire school, by user, or by group.
    - Enforce granular usage policies—for example, allow certain social media applications on school-owned computers while denying the chat feature, or allow file downloads while denying file uploads to file sharing and storage apps.
    - Identify and block proxy technologies, such as Tor, Ultrasurf, and PHProxy, designed to circumvent port-and-protocol firewalls, web filtering technologies, and proxy servers.

- **SSL Decryption:** All Palo Alto Networks firewalls perform decryption, improving visibility into potential threats while eliminating the management overhead and performance impact of separate decryption appliances. Schools can:
  - Decide which inbound and outbound traffic to decrypt based on URL categories, source users, and source/destination IP addresses.
  - Decrypt traffic in virtual wire, Layer 2, or Layer 3 mode, and even decrypt HTTP/2 streams, maintaining performance benefits instead of downgrading sessions to HTTP/1.1.
  - Inspect decrypted traffic for threats and apply security policies.
  - Create a copy of decrypted traffic and send it to a traffic collection tool for archiving and analysis using the Decryption Port Mirror capability.
- **Threat Prevention:** This subscription for Next-Generation Firewalls eliminates evasive threats at every stage of an attack, preventing exploits from reaching devices, disrupting command-and-control traffic, and enforcing IPS protections across all ports and protocols.

Exceed Compliance with Best Practices

Schools should strongly consider configuring these capabilities to stop new and evolving threats from traversing the network, exfiltrating sensitive data, or allowing inappropriate content to find its way to minors. With thousands of new websites created every day, the only way to prevent threats or inappropriate content from reaching schools and students is realtime, automated protection. Some school districts monitor school-owned devices for CIPA compliance even after the devices have left the school network, while others only monitor within school boundaries. Either way, schools must extend security policies to school-owned devices, including 1:1 devices. Palo Alto Networks Next-Generation Firewalls can help in multiple ways:

- **Zero-day threat prevention**, enabled by WildFire® malware prevention service, automatically detects and stops unknown threats that would harm minors or steal data. Realtime data from the world's largest threat intelligence sharing community rapidly identifies unknown threats, and the service automatically delivers protections in as few as five minutes after a threat is discovered anywhere in the world. WildFire works with URL Filtering to automatically block brand-new inappropriate or malicious URLs.
- **Remote security**, enabled through a subscription to GlobalProtect™ network security for endpoints or Prisma™ Access, secures mobile device and branch location traffic flows to data center and cloud applications with IPsec/SSL VPN tunnels. It can apply the same, consistent security policies to school-owned devices, including laptops, tablets, and more.
- **Data filtering profiles** prevent sensitive information, such as credit card and Social Security numbers, from leaving a protected network. You can filter keywords that signal harmful or threatening content for certain applications or file types.
- **Zero Trust network segmentation** protects sensitive data and traffic flows within your organization, ensuring valid users have access to the resources they need while denying all others. It also prevents malware from spreading from untrusted networks to critical applications, such as from school wireless networks to the data center. Network segmentation works in conjunction with URL Filtering, App-ID, User-ID, data filtering, and remote device security to consistently secure your most sensitive data and applications.
- **Credential theft prevention** stops your users from submitting passwords to unknown sites, works with URL Filtering to block access to known phishing sites, and stops hackers from using stolen credentials to gain access to your systems.
- **DNS Security service** applies predictive analytics, machine learning, and automation to block misuse and attacks that use DNS, and eliminates the need for independent tools.

More Information

For more details about Palo Alto Networks technology and how we secure education, see these resources:

- Read about our work with K-12 schools.
- Learn about our industry-leading Next-Generation Firewalls.
- Understand how our offerings support the E-rate Program.
- See how our Next-Generation Firewalls decrypt web traffic in a K-12 environment.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com