How Palo Alto Networks Can Help Address CIPA Requirements

OVERVIEW

The Children's Internet Protection Act (CIPA), is a federal law enacted by the United States' Congress in December 2000 to address concerns about access in schools and libraries to the Internet and other information. CIPA imposes certain requirements that are tied to discounts for Internet access or for internal connections that a school or a library may receive. Further, in early 2001, the Federal Communications Commission (FCC) issued additional rules to ensure that CIPA is carried out.

CIPA REQUIREMENTS

The complete list of requirements that schools and libraries must meet in order to be CIPA compliant are defined at www.fcc.gov. Several of the key requirements are summarized below:

- **Web Filtering:** Schools and libraries subject to CIPA cannot receive the discounts offered by the "E-Rate" program (discounts that make access to the Internet affordable to schools and libraries) unless they certify that they have certain Internet safety measures in place. These include measures to block or filter pictures that: (a) are obscene, (b) contain child pornography, or (c) when computers with Internet access are used by minors, are harmful to minors;
- **Monitoring Online Activity of Minors:** Schools subject to CIPA are required to adopt a policy to monitor online activities of minors;
- **Policy Implementation:** Schools and libraries subject to CIPA are required to adopt a policy addressing: (a) access by minors to inappropriate matter on the Internet and World Wide Web; (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. CIPA does not require the tracking of Internet use by minors or adults.

Schools and libraries are required to certify that they had their safety policies and technology in place before receiving E-rate funding.

HOW PALO ALTO NETWORKS ADDRESSES CIPA COMPLIANCE REQUIREMENTS

Palo Alto Networks' next-generation firewall uses three innovative technologies that allow schools and libraries to regain visibility and control over applications, users and content traversing their network. These technologies, App-ID, User-ID and Content-ID, bring the business-relevant elements of applications, users and content under policy control using a high performance firewall architecture.

- **App-ID** is a patent-pending technology that identifies and controls more than 1,200 applications irrespective of port, protocol, SSL encryption, or evasive tactic employed. App-ID can help reign in today's students who are Internet experts and are increasingly using a new class of application that can easily circumvent existing security mechanisms such as firewalls, URL filtering and proxy servers.

  These applications, which include TOR, UltraSurf and PHproxy, put IT departments in a difficult position. State and Federal regulations, school board policies, community standards, and common sense dictate that schools filter applications and Internet traffic that can make its way to students' eyes and ears.

The conventional approach to solving this problem includes deploying a URL database in conjunction with a traditional network firewall, but this approach simply can't keep pace with these nimble, network-savvy applications. Today, it alone is no longer enough.

The solution is to use Palo Alto Networks and App-ID to identify the application first and foremost. Armed with the knowledge of which applications are traversing the network, IT departments can enable policies that foster education and research yet control access to the applications and content that may threaten CIPA benefits.

- **User-ID** is a technology that integrates Palo Alto Networks next-generation firewalls with Microsoft Active Directory, LDAP, eDirectory and Citrix resulting in visibility and control of applications based on users and groups – not just by IP addresses. In Citrix and terminal services environments, User-ID can associate the individual user with their network activity, enabling IT to control applications based on users that are normally obfuscated by a Citrix server. CIPA's requirement to monitor the access of minors can be addressed through a security policy that is based on user and group information from Active Directory. This association of all traffic with users and groups allows for IT staff:
  - Regain visibility into user activities relative to the applications in use and the content they may generate.
  - Tighten security posture by implementing policies that tie application usage to specific users and groups, as opposed to simply the IP address. Student policies can be different than Faculty, Administration, or even IT.
  - Identify Citrix and Microsoft Terminal Services users and control their respective application usage. These tools, while allowing for multiple users to share resources are also common grounds for misuse. A single terminal server might support tens to hundreds of users/students. Again, visibility into the actual distinct users and their group membership allows for consistent policy enforcement and compliance.
- **Content-ID** is a content inspection engine that prevents a wide range of threats, blocks unauthorized file and data transfers and controls web surfing. The Internet can invite, infect, and corrupt the unsuspecting user and as such, protection against these pitfalls is critical to CIPA compliance. Palo Alto Network's next-generation firewall protects against the unauthorized disclosure, use, and dissemination of personal information regarding minors via viruses, spyware, and vulnerability exploits through the use of a uniform threat signature format and stream-based scanning architecture. The uniform signature format means that traffic is inspected only once—as opposed to the multiple scans that most other solutions must execute. Stream-based scanning means that the content scanning process begins as soon as the traffic is received.

  Palo Alto Network's URL Filtering service combines an on-box dataset with a hosted service that ultimately provides access to information on over 200 million websites- ten times more than the current market leaders. This allows schools and libraries to manage Internet access to over 70 URL categories including Adult Material, Questionable, Hacking and other topics pertinent to CIPA. The dataset also maintains an up to date and comprehensive list of proxy websites in the Proxy Avoidance, and Anonymizers category, mitigating the exposure to inappropriate material accessed through this class of websites.

All of this technology runs on a high-performance, purpose-built platform based on Palo Alto Networks' Single-Pass Parallel Processing (SP3) Architecture. Unique to the SP3 Architecture, traffic is only examined once, using hardware with dedicated processing resources for security, networking, content scanning and management to provide line-rate, low-latency performance under load. Best of all, the solution complements other infrastructure technologies and can easily be deployed in virtual wire (in-line) or as a firewall.

SUMMARY

Palo Alto Networks next-generation firewalls can help schools and libraries achieve and maintain CIPA compliance while simultaneously protecting students and users from unscrupulous Internet criminals.