Child Internet Protection Act and More: Create a Safe and Secure School Environment in a Post-PC Era
Child Internet Protection Act and More: Create a Safe and Secure School Environment in a Post-PC Era

What You Will Learn

Most schools comply with Children’s Internet Protection Act (CIPA) using a web-filtering appliance. But the appliance addresses only one of many aspects of security of modern schools, which also need to prevent malware, keep students from illegally sharing copyrighted music and video, and control network access when students and teachers bring their own devices to school.

This white paper, intended for school administrators, board members, and IT teams, explains the value of Cisco® security solutions for schools in this post-PC era:

• With one investment, you can provide CIPA compliance as well as malware protection, prevention of illegal file sharing, support for a bring-your-own-device (BYOD) policy, and more.
• Consolidating security devices lowers capital and management costs.
• The Cisco Security Intelligence Operations (SIO) center provides industry-leading protection against malware.

New Challenges in School Security

Your school’s current web-filtering solution helps to meet CIPA requirements by blocking web traffic by category, such as hate groups, gambling, or pornography. This is a solid first step, but web filtering does not block other undesirable Internet traffic that can harm students or the school network. Schools also need the ability to:

• Stop websites from surreptitiously installing malware onto school-owned devices. Many seemingly legitimate sites infect computers, enabling hackers to extract confidential information such as grades or salaries, or to bring down the network.
• Prevent students from sharing copyrighted music and video files over the district network.
• Support a BYOD policy, allowing students and faculty to connect to the campus network from personal laptops, tablets, smartphones, and other devices. Schools typically configure school-owned computers to use search engines’ “safe search” option to block adult content from search results. How can they enforce this policy on personal devices used on campus?
Child Internet Protection Act and More: Create a Safe and Secure School Environment in a Post-PC Era

Cisco Security Architecture for Schools

Schools can address multiple security requirements with one investment in a Cisco security architecture, reducing capital, management, and training costs compared to investing in multiple single-purpose solutions.

Comply with CIPA

**Challenge:** CIPA imposes requirements on schools or libraries that receive funding support for Internet access or internal connections from the E-rate program.

**Solution:** Cisco Adaptive Security Appliance (ASA) CX Context-Aware Firewall meets all CIPA safety requirements. It blocks or filters Internet access to inappropriate images and content. It monitors students’ online activities and addresses safety and security concerns when minors use email, chat rooms, or other electronic communications. Cisco ASA CX Firewall also helps to thwart unlawful activities such as hacking, and to prevent leakage of personal information regarding minors.

The Cisco security architecture even helps to consistently block adult content from search engine results. While Google, Bing, YouTube, Flickr, and other popular search engines and content-sharing sites provide a safe-search option to keep adult content from being presented in results, savvy students can easily turn off the option on school-owned and personal devices. Schools can transfer control of the safe-search option from students to administrators by selecting the safe-search option on the Cisco Web Security Appliance. This makes all search requests initiated from the school network appear to be safe-search requests.

Most web-filtering solutions for CIPA are comparable. Uniquely, the Cisco ASA CX Firewall also addresses other important school security requirements, described in the following paragraphs.

Protection from Even the Newest Malicious Websites

Cisco Security Intelligence Operations (SIO) keeps schools protected and informed about emerging threats that could take down the network or enable hackers to retrieve confidential information. Schools benefit from the US$100 million Cisco invested in the SIO:

- Cisco SensorBase is a threat-monitoring network that captures threat telemetry from over 700,000 Cisco sensors deployed globally, monitoring 35 percent of the world’s email and web traffic. This live data is combined with a historical database of more than 40,000 vulnerabilities.
- Cisco Threat Operations Center is staffed by 500 security analysts as well as automated systems. The analysts conduct research on emerging threats 24 hours a day, every day, from offices throughout the United States as well as Australia, China, India, Israel, Ukraine, and the United Kingdom.
- Dynamic updates are delivered to your Cisco security devices within a few minutes, often hours before other solutions, protecting the school network against the latest threats.
Block Malware, Saving Time and Costs of Remediation

Challenge: School computers and networks can become infected when students, teachers, and staff visit legitimate-seeming websites that are actually malicious. For example, in 2009, it was widely reported that fans searching online for actress Jessica Biel had a one-in-five chance of hitting a website with malicious code that could affect their devices or network. Investing in web security pays dividends for schools because it avoids the high costs of IT staff time and consultants to remediate infected computers and restore down networks.

Solution: Cisco security solutions apply multiple techniques to block access to malicious websites. Like other solutions, they block websites already known to have undesirable content. What sets them apart is how effective they are in blocking websites not yet reported as being malicious. One way they achieve this is by connecting with the Cisco Security Intelligence Operations (SIO) service, which calculates a reputation score for websites by considering years of operation, ownership country, history of ownership, and more. Websites or individual objects on websites with negative scores are blocked. Other methods include blocking attempts by the site to install malware; warning school users when they click a link to a website that looks suspicious; and enforcing common-sense policies such as blocking transfer of files over a certain size, often audio or video files.

Prevent Illegal Sharing of Copyrighted Material

Challenge: Schools need to prevent students from sharing copyrighted material such as music and video files, a type of Internet traffic known as peer-to-peer file sharing. Simply prohibiting file sharing on school-owned computers is not enough because students increasingly bring their own devices (laptops, tablets, and smartphones) to school.

Solution: Rather than configuring each device to prevent peer-to-peer file sharing, schools can select this option on the Cisco ASA CX Firewall. The ASA CX enforces the policy regardless of whether the student is using a school-owned or personal device.

Block or Allow Individual Features on Social Networking Sites

Challenge: Some schools want to allow use of social networking sites such as Facebook for group collaboration, but to block individual features such as games or chat.

Solution: Configure the Cisco device to block specific application features.

Control Guest Access in a BYOD World

Challenge: School visitors, including parents, board members, and special presenters, increasingly expect guest wireless access. But schools generally want to limit their access to browsing and checking email, keeping them off the network used for student information systems and other internal systems.

Solution: Cisco Identity Security Engine (ISE) can automatically register guests, restricting traffic to a guest VLAN that provides Internet access only. The school IT team does not have to spend time issuing passwords.
Child Internet Protection Act and More: Create a Safe and Secure School Environment in a Post-PC Era

Why Cisco?
Schools strengthen protection against unwanted Internet activity (browsing adult content, malware installation, and peer-to-peer file sharing) by implementing a Cisco security architecture. This is because Cisco takes a holistic view of security, using all network devices, including switches and routers, to enforce an access policy instead of developing individual systems that work in isolation.

The difference is that with a Cisco security architecture, you can grant students’ and teachers’ requests based on the context: who is asking, what device they are using, how they are connecting (wired, wireless, or remote), when, and where. For example, if a student attempts to visit the web from a tablet, the Cisco architecture can detect whether the device is school-owned or personal, and communicate this information to the network infrastructure so that it can enforce the appropriate access policy.

Cisco security architecture provides better protection and more flexible policy enforcement than so-called next-generation firewalls. For example, the school IT team can restrict or block access to all services for a student who tries to hack into school databases or repeatedly attempts to access blocked sites on the school network as well as the Internet. The team can also selectively grant access in certain school systems to individual teachers and administrators.

The technology behind this flexibility is the Cisco Identity Services Engine (ISE). The school IT team indicates the user’s privileges in just one place, the Cisco ISE. Then, when the user is authorized, that user’s traffic is tagged to instruct all other network devices to block it or pass it through.

Conclusion
When evaluating CIPA solutions, schools can increase their return on investment by looking for an architecture that also address other looming security challenges, including malware blocking, peer-to-peer file sharing, access control in a BYOD world, and guest access.

The Cisco security architecture addresses all of these security requirements, meeting the needs of the modern school community.
For More Information

To learn more about Cisco security solutions for schools, visit:

To learn more about Cisco solutions for education, visit:
www.cisco.com/go/useducation.