

INDUSTRY SECURITY

- **Control web content** to protect students and achieve CIPA compliance
- **Secure communications** with integrated IPSec and SSL VPN capabilities
- **Protect confidential student information** from unlawful access and spyware
- **Implement strong identity management** through sophisticated authentication options
- **Restrict rogue endpoints** so only authorized computers can connect to the network



Earth-friendly technology

Protecting an Education Network

From K-12 through higher education, there are consistent themes in network security that are of universal concern – connectivity, protection from malware, protection from harmful content, and increasingly the collection of forensic data.

At the K-12 and library level, there is an additional incentive driving network security. For schools and libraries to be eligible for the Federal Communications Commission Universal Service Fund (commonly known as “E-Rate”), the Children’s Internet Protection Act (CIPA) requires that they adopt an Internet safety policy and employ protections that block or filter visual depictions deemed obscene, pornographic, or harmful to minors.

Security Challenges Faced by the Education Community:

Whether at the state, district, campus or faculty level, these are common computer and network challenges faced by all members of the education community:

- **User authorization** - All schools must ensure that *only* authorized users have access to computing and network resources.
- **Protection against malware and harmful content** - The number of ways that malware and harmful content can enter the network is ever increasing. Attacks can come via email and web surfing, and also through the growing use of Instant Messaging (IM) and Peer to Peer (P2P) applications. This is the area that CIPA was created to address.
- **Secure communication** - Whether supporting teachers who want to access network resources from home, or providing secure communications between facilities across public networks, the need for Virtual Private Networks (VPN) is critical.
- **Managing integration of rogue endpoints** - Many schools have policies that prohibit bringing laptops to school. Students, teachers and staff, however, still find ways to plug their personal equipment into the school network. This presents the risk of spreading malware within the network, as well as the threat of data leakage. The problem is further exacerbated for those schools that choose to deploy wireless networks, especially with the growth in handheld devices that come with Wi-Fi capabilities.
- **Forensics** - Even with acceptable usage policies in place, it is still necessary for schools to monitor their networks in order to identify unauthorized intrusion attempts and to track the usage of authorized users to ensure that they are adhering to the terms of the policy.

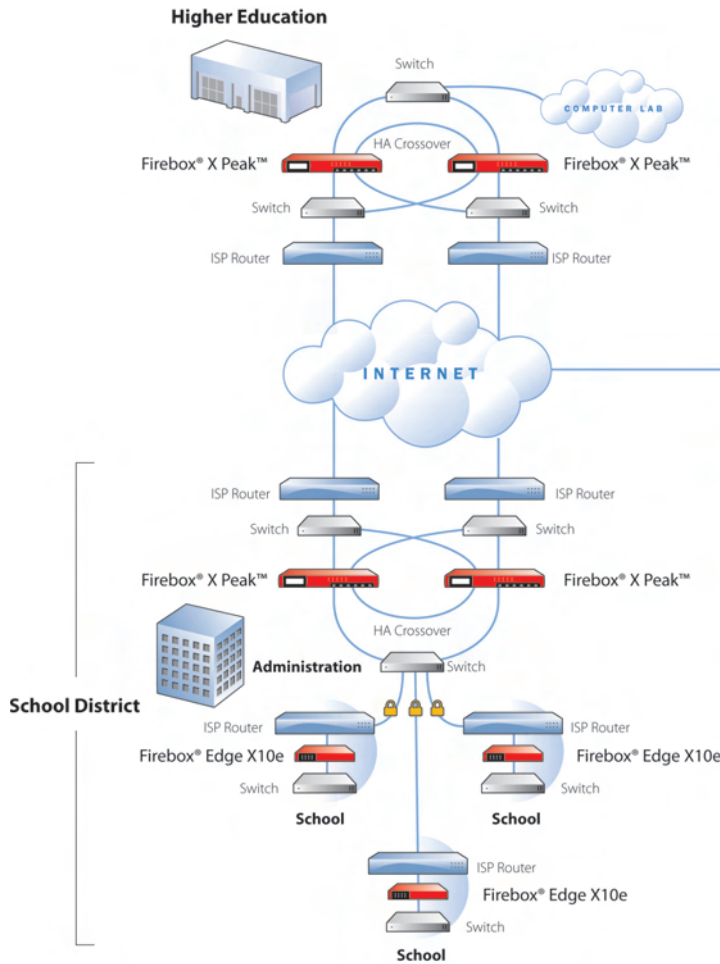
Network Traffic Logs – the Key to Network Forensics

All WatchGuard XTM appliances provide a range of network traffic and user authorization logging capabilities. For verbose diagnostics, either syslog or the WatchGuard proprietary formats may be used for collecting network traffic data. In addition, integration with standard network monitoring solutions can be achieved via the XTM SNMP support.



Extensible Threat Management for Education

Extensible threat management (XTM) security solutions from WatchGuard aggregate multiple security measures into a single, easily configurable solution. Choose from a family of these devices, which can be deployed everywhere from individual schools to district or state data centers. XTM protects school data while delivering reliable management, monitoring, logging, and reporting.



WatchGuard offers a family of interoperable, centrally managed devices appropriate for everything from a small private school to large campuses and multi-site education networks.

Identity Management

With built-in authorization databases or the option of integrating with Active Directory, LDAP or RADIUS, the WatchGuard XTM solutions provide a range of sophisticated user authorization capabilities. This helps to ensure that only authorized students and teachers can access computer and network resources. It also allows school acceptable usage policies to be reinforced by providing detailed control over those applications and services that users are able to access.

Address Content Control

K-12 schools in particular require detailed control of the content that students are allowed to access for CIPA compliance and to meet their Acceptable Usage criteria. WatchGuard WebBlocker security subscription provides detailed URL filtering capabilities on HTTP and HTTPS, with no per user licensing fee.

HTTPS URL filtering helps to eliminate many of the more popular techniques for getting around content filtering. With WatchGuard's proxy firewall architecture it is also possible to prohibit the use of IM and P2P applications, helping to reduce the potential for exposure to harmful content and incoming malware. Combining this content filtering with the ability to prohibit the ingress of malware via the Gateway AntiVirus/Intrusion Prevention Service and spamBlocker security subscriptions provides the ultimate in content control.

Secure Communications

Integrated into all WatchGuard XTM appliances is support for Virtual Private Networks (VPN) via IPSec, which provides secure site-to-site communications. In addition, mobile users have access to secure communications via either IPSec or SSL VPN.

Manage Rogue Endpoints

For wired or wireless networks, WatchGuard XTM appliances can be configured to ensure that only authorized computers are allowed access to the network. The ability to create network zones for wireless networks also provides the maximum in network protection with the flexibility of wireless guest network access.

For more information about WatchGuard Education Security Solutions, contact your reseller, visit www.watchguard.com, or call the number below.

Address: 505 Fifth Avenue South, Suite 500, Seattle, WA 98104 • **Web:** www.watchguard.com • **U.S. Sales:** 1.800.734.9905 • **International Sales:** +1.206.613.0895

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. ©2008 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, Firebox, LiveSecurity, Peak, and Core are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE66574_091108

