Securing K-12 Wireless Networks

Schools are struggling to balance the advantages of wireless access with inherent security threats. SonicWALL delivers a secure distributed wireless solution for academic environments.

CONTENTS

SONICWALL®

Abstract

Wireless networking is being incorporated into many educational environments to add flexibility and increase productivity. This paper examines security issues to consider when evaluating security solutions for academic wireless networks. The SonicWALL Secure Distributed Wireless Solution offers schools and school districts with a comprehensive, cost-effective approach to implementing and extending wireless academic networks.

Cutting the Cord: Wireless Security Considerations

Wireless Internet access is rapidly becoming commonplace in schools. Forty-five percent of U.S. public schools with Internet access used wireless connections in 2005, an increase from 32 percent in 2003.[1] Wireless access over a growing number of increasingly mobile device types, including laptops, PDAs and smartphones, while enhancing flexibility in communications and collaborative learning, can expose schools to security breaches, denial of services, and regulatory noncompliance. Schools need to be selective in evaluating wireless solutions that provide appropriate protection, without burdening resources or budgets.

Evaluating Wireless Equipment

Not all wireless equipment is created equal. Consumer-grade products, while offering simplicity and lower purchase price, can lack needed security, intelligence, central management and WLAN integration. Considerations for evaluating a wireless solution include total cost of ownership, processing power, scalability, advanced security features, transmission power and ease of deployment.

Connectivity Concerns

Open wireless traffic is like a radio broadcast: if you are in range, you can receive the signal, whether you should or not. Some security protocols, such as WEP and WPA, are easily hacked. Wireless security requirements should include user authentication, data encryption, proven security technologies (e.g., IPSec, SSL VPN), security zoning and support for corresponding 802.11 standards.

Ensuring Data Integrity on Mobile Devices

Because they are less under the direct control of the school's IT department, laptops and other mobile devices expose schools to additional threats from Trojans, worms, viruses, spyware and other malware. A wireless solution should stop harmful threats before they enter the school network. It should also block inappropriate Web sites and peer-to-peer applications that expose school networks to malware, violate compliance regulations, risk legal liability, and sap bandwidth and productivity.

Streamlining User Experience

Problems occur when dropped connections or cumbersome applications lead users to take matters into their own hands, purposefully or inadvertently disabling security features, bypassing crucial security steps, and even installing rogue access points of their own. Wireless solutions should be noncomplex and intuitive, with simple interfaces, simple procedures and streamlined roaming functionality.

Easing Management

Security should not disproportionately increase IT administration. Typical wireless solutions are "point solutions" that require a dedicated switch or wireless controller, and a different interface for deployment, configuration and management. Separate networks for wireless double the demand on resources for design, policy configuration, deployment and administrative updates. A single integrated solution for both wired and

---

[1] U.S. Department of Education, National Center for Education Statistics (2006). Internet Access in U.S. Public Schools and Classrooms: 1994-2005 (NCES 2007-020).

wireless networks is preferred to enforce current policies, monitor and analyze activity, and respond to attacks.

SonicWALL Secure Distributed Wireless Solution

The SonicWALL® Secure Distributed Wireless Solution is the first total security solution that integrates 802.11a/b/g wireless management and security enforcement into an enterprise-class firewall/VPN appliance. The SonicWALL Secure Distributed Wireless Solution is built around our award-winning line of network security appliances in combination with SonicPoints™ to extend secure wireless coverage across the network.

SonicWALL UTM Wireless Controllers

Acting as a wireless LAN controller SonicWALL® TZ, NSA, and E-Class NSA Series network security appliances automatically detect and configure SonicPoints, dependent access points, as they are added to the network while simultaneously enforcing security policies on all wired and wireless traffic. This eliminates the need for a separate wireless appliance at the network perimeter, provides airtight wireless mobility for students, staff and teachers, and enables secure Internet access for guests.

SonicWALL all-in-one network security solutions provide school networks with an expanding array of customizable integrated Unified Threat Management (UTM) services featuring high-speed deep packet inspection (DPI). DPI prevents malicious attacks that can penetrate stateful packet inspection firewalls. SonicWALL UTM solutions deliver intelligent, real-time network security protection against sophisticated application-layer and content-based attacks, including viruses, spyware, worms, phishing attacks, Trojans, software vulnerabilities such as buffer overflows, and bandwidth and Internet misuse.

SonicWALL SonicPoints

Available in IEEE 802.11a/b/g and 802.11b/g options, SonicPoints are dependent access points that provide secure wireless LAN connectivity to users on the network. There is no need for a separate wireless appliance at the perimeter. Because wireless access is delivered as part of the SonicWALL network security appliance, the wireless network enjoys the same UTM protection as the rest of the network. The SonicWALL Secure Distributed Wireless Solution also supports Wireless Guest Services (WGS) throughout the network, and uninterrupted roaming between SonicPoints.

Utilizing the Virtual Access Point (VAP) feature, SonicPoints can broadcast up to eight distinct SSIDs with dedicated authentication and privacy settings while sharing the same physical infrastructure. SonicPoints require no pre-configuration, as they are centrally configured, managed and updated by any SonicWALL network security appliance. By streamlining wireless deployment and policy enforcement, SonicWALL reduces demands on limited IT resources and lowers total cost of ownership. SonicWALL supports standards-based Power over Ethernet (PoE) automatically to SonicPoints or any other 802.3af-compliant appliance.

SonicWALL SRA: Clean VPN for Mobile Devices

Mobility is crucial to many educational environments that have temporary facilities, specialized instructors who travel between multiple school sites, or faculty and administrators who require access to school resources from home or on the road. SonicWALL network security appliances configured as wireless LAN controllers can also be deployed in conjunction with next-generation SonicWALL Secure Remote Access (SRA) technology to create a SonicWALL Clean VPN™. This configuration enforces granular application-layer access policies while comprehensively inspecting all traffic at the gateway, all the while correlating event information to streamline and enhance security efficiencies.

SonicWALL SRA solutions include the SonicWALL SSL VPN Series and the SonicWALL Aventail® E-Class SSL VPN Series. SonicWALL SRA solutions deliver flexible, scalable cross-platform solutions for wireless networking, secure remote access, disaster recovery and secure extranets. They extend clientless mobile access over standard Web browsers to laptops, wireless PDAs and smartphones with unsurpassed granular control. Additionally, SonicWALL network security solutions feature integrated site-to-site IPSec VPN functionality.

SonicWALL CFS: Robust Content Filtering

SonicWALL Content Filtering Service™ (CFS) is engineered to help meet the regulatory demands of the Children's Internet Protection Act (CIPA). The flexibility of SonicWALL CFS to block proxy-based applications (e.g., YouTube, etc.), and the ability to set custom policies for different groups or different times of day, makes it ideal for educational settings.

In addition to legislation such as CIPA, SonicWALL CFS is an integral part of internal compliance programs designed to reduce the liabilities that may be incurred when inappropriate content is allowed into the network. When Web access is unrestricted, not only is the result counter-productive, it can also result in costly lawsuits. SonicWALL CFS enforces protection and productivity policies by employing an innovative rating architecture, utilizing a dynamic database to block up to 56 categories of objectionable Web content, while maximizing throughput.

SonicWALL GMS: Centralized Management and Compliance Reporting

The reporting necessary to comply with today's academic regulatory mandates can be fulfilled by the SonicWALL Global Management System (GMS™) and ViewPoint™ reporting package. GMS provides schools and districts with a flexible, powerful and intuitive tool to globally manage SonicWALL appliances and security policy configurations over LAN, WAN and wireless networks for gateway anti-virus, anti-spyware, intrusion prevention and content filtering, all from a single central console, resulting in faster deployments and lower IT overhead.

SonicWALL ViewPoint is an easy-to-use Web-based reporting tool that fully compliments and extends SonicWALL's security products and services. Using both a customized dashboard and a variety of historical reports, ViewPoint provides academic IT administrators with insight into the health of their network including network utilization, security activity and Web usage.

Conclusion

Wireless technology will continue to be integrated into academic environments. Schools need to keep pace with wireless security in order to protect both their data resources and their students. The SonicWALL Secure Distributed Wireless Solution provides an easy-to-deploy, scalable and comprehensive wireless security solution for schools and school districts of any size.