The K-12 Budget Case for Internet Security

While Internet access has expanded, school budgets have tightened. To protect investments and resources, schools must apply limited funds strategically.

CONTENTS

SONICWALL®

Abstract

School budgets have not kept up with the explosive pace of instructional Internet access, or the corresponding threat to academic and administrative resources. This paper explores trends in academic Internet use, the budgetary arguments for greater information security, and funding considerations unique to academic environments. SonicWALL solutions provide powerful, granular and complete security solutions that reduce the cost and complexity of running educational networks.

Security Threats are Budget Threats

The Internet has become an intrinsic component of education. As of 2005, among U.S. public schools[1], nearly 100% had Internet access, with 94% providing access into instructional rooms. Of those, 45% used wireless. The ratio of students to Internet-connected instructional computers was 3.8 to 1.

At the same time, academic applications of the Internet have become more sophisticated. Schools host their own Web sites. Teachers use e-mail when communicating with students and parents. Shared instructional material and e-learning tools are being delivered online to satellite classrooms, homes and computer-based training (CBT) centers. Administrative functions such as assignment boards, activity boards, applications and scheduling services are now hosted online by third-party providers. Districts employ point-to-point or virtual private networks (VPNs) between schools. Students, teachers and parents routinely access the Internet from a growing number of increasingly mobile device types, including laptops, PDAs, and smartphones.

The revolutionary pace of technology has exposed schools to security breaches, bandwidth piracy, automated denial-of-service attacks, and regulatory liability associated with access to unacceptable or illegal materials. Critical and sensitive data is prone to illegal access, loss or alteration, often in violation of privacy regulations.

Yet while academic Internet access has expanded rapidly over the last decade, budgets have only gotten tighter. In order to protect academic and administrative resources, IT needs to apply limited funds more strategically and intelligently than ever.

Protecting technology investment

A school's network is only as valuable as the data and applications it contains. Increasingly profit-oriented and criminal attackers prey on students and faculty to introduce malware into school networks and gain access to sensitive resources. Compromised security can devastate a school's mission-critical resources and disrupt academic activity.

Threats have grown more varied and sophisticated. Worms and viruses slow down infected systems and networks, corrupt files and applications, and steal bandwidth, often e-mailing themselves to everyone in a user's contact lists or installing a back door on the infected computer that can later be used by spammers or to infect other traffic on the network. Trojan horses and bots disguise themselves as popular shareware programs, pictures or music files, so that students feel safe launching them. Both Trojan horses and bots may be dormant until a predefined event occurs and then are controlled by a remote hacker. Additional risks come with wireless networks, since hackers just outside of the physical school boundaries can eavesdrop on traffic or access shared files. Furthermore, sophisticated hackers can easily defeat Wired Equivalent Privacy (WEP) security features turned by exploiting its widely publicized security flaws.

[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).

Maximizing return on investment (ROI)

No security solution is worth the price if it cannot deliver the performance needed to add operational value. To provide maximum return on a school's overall technology investment, a security solution should not come at the cost of clogged bandwidth, network downtime, restricted communications, reduced productivity or overburdened IT resources. Instead, it should be engineered to eliminate bottlenecks and streamline processes to deliver protection transparently to academic and administrative operations.

Safeguarding against liability

The Children's Internet Protection Act (CIPA) calls for schools to install Web filtering technology to protect students from offensive, exploitative or otherwise dangerous material, which also protects school networks from attack. Many of the sites that are blocked at the source not only host material that may be offensive, they also host malware and spyware that can easily infiltrate school networks.

Cutting costs by cutting complexity

In challenging economic times, schools must do more with less. In selecting a security solution, greater complexity has a direct correlation with greater costs related to management, administration, training and user support. Unfortunately, many traditional "status quo" vendors continue to offer solutions of greater complexity and cost, but without correspondingly greater value. By ineffectively allocating diminishing IT budget resources on overly complex solutions, schools run the risk of underfunding other crucial security initiatives. To prevent this oversight, as an alternative to over-priced and overly-complex vendors, schools must seek out simpler, streamlined security solutions that do not compromise performance or effectiveness.

Funding Considerations

A school's security solution choice should be driven by need, not by funding source. However, the more schools know about funding options, the better able they are to stretch their security budgets. For example, different funding may be appropriately applied to one-time costs (e.g., upfront purchase, implementation, integration, initial training) and ongoing costs (e.g., administration, maintenance, support, incremental training). Funding sources including E-Rate funding; tax-exempt lease purchases; bonds and targeted tax referenda; state and federal grants and appropriations; and donations and grants from corporations and foundations. Correspondingly, security solutions can be implemented as one-time or recurring expenses (the latter being particularly applicable to managed security services). These expenses can then be tied to appropriate funding sources that may be specific to a particular fiscal year or bridge multiple years.

E-Rate

The E-Rate program ("The Schools and Libraries Universal Service Fund") was created as part of the Telecommunications Act of 1996 to ensure that all eligible K-12 schools (public and private) and public libraries in the United States have affordable access to modern telecommunications and information services. E-Rate provides eligible schools with support for both one-time and ongoing expenses related to information security. E-Rate recipients are required to comply with CIPA regulations.

Tax-exempt lease purchase

A tax exempt lease purchase (TELP) is an installment-based financing arrangement available to public schools and districts that can be applied to technology purchases. The school retains ownership and equity. Usually, the interest portion is tax-exempt. TELP is commonly used for acquiring a variety of asset types, including computers and equipment. TELP can help schools takes full advantage of tax-exempt status, and allow security solutions to be put in place immediately instead of waiting for full funding availability.

Time-sensitive funding

Generally, the funding source should match the life span of the equipment. For instance, tying purchase of equipment with an anticipated 7-year lifespan to a 15-year bond would be inadvisable, because the school would be paying for the equipment long after its useful life.

SonicWALL Solutions for Education

SonicWALL® is committed to providing schools of all size with cost-effective security solutions, which deliver equal or greater value at a significantly lower total cost of ownership when compared with competitive solutions. SonicWALL is uniquely positioned in the industry to eliminate costs out of building and running secure high-performance networks by reducing costs associated with:

- Operational performance—by delivering high-performance real-time security solutions that integrate leading-edge software intelligence with high-performance state-of-the-art commercially available chipsets, delivered on industry-standard hardware platforms;
- Implementation—by providing "hands-off" integrated solutions that simplify setup and distribution while seamlessly fitting into even the most demanding network infrastructures; and
- Management—by delivering intuitive, globally-managed and centrally-administered control.

SonicWALL solutions do not sacrifice performance for cost-efficiency. SonicWALL engineers take the complexity out of information security, freeing school resources to enhance productivity and learning.

SonicWALL network security: Comprehensive malware protection

SonicWALL® all-in-one TZ, NSA and E-Class NSA Series network security solutions provide school networks with an expanding array of customizable integrated Unified Threat Management (UTM) services. Malicious attacks can penetrate stateful packet inspection firewalls. SonicWALL network security 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 Application Firewall adds highly-configurable controls to prevent data leakage and manage bandwidth at the application level. SonicWALL can provide dynamic network protection through continuous, automated security updates, protecting against emerging and evolving threats, without requiring any administrator intervention.

SonicWALL RFDPI: ultra high-performance UTM architecture

At the heart of every SonicWALL network solution is its revolutionary high-speed Reassembly-Free Deep Packet Inspection™ (RFDPI) technology (U.S. Patent 7310815). Unlike other "proxy" solutions, SonicWALL's real-time RFDPI can analyze files and content of any size with extremely low latency, without reassembling packets or application content, resulting in extremely high-speed performance. This is far superior to the stateful packet technology employed by other firewalls.

Additionally, SonicWALL NSA and E-Class NSA solutions feature ultra high-speed multi-core processors to deeply protect any size academic network with uncompromising performance. SonicWALL multi-core load balancing enables applications, files and content-based traffic in multiple streams to be inspected simultaneously, with no significant impact on performance or scalability.

SonicWALL Content Filtering Service: Robust content filtering

The Children's Internet Protection Act (CIPA) requires all schools and libraries that receive E-Rate funding to install content filtering. SonicWALL Content Filtering Service (CFS) is engineered to help meet those legislative demands. 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 Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service: Highly-effective intrusion prevention

Many of the most dangerous threats to educational networks function at the application layer, exploiting vulnerabilities in common network applications to drain productivity and steal data. The SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service scans for worms, Trojans, software vulnerabilities, backdoor exploits and other types of malicious attacks. Working in conjunction with SonicWALL anti-virus and anti-spyware technology, the SonicWALL engine protects against an array of network-based application vulnerabilities and exploits. Deployed to protect against both internal and external threats, SonicWALL network security solutions monitor the network for malicious or anomalous traffic, then blocks or logs traffic based on predefined and automatically updated conditions. By focusing on known malicious traffic, SonicWALL decreases false positives while increasing network reliability and performance.

SonicWALL Secure Distributed Wireless: Making wireless secure and affordable

Wireless networking offers many benefits for schools, from a cost-effective means of extending network access to enabling maximum student access to information resources. Yet the management and security challenges are considerable.

With a SonicWALL security appliance acting as a gateway for up to 128 wireless access points, the management and security of a school's wireless network can be handled on the same platform used for your wired network.

SonicWALL also offers higher levels of wireless security, allowing the enforcement of robust SSL VPN for all wireless traffic. Rogue access point detection neatly eliminates another wireless security backdoor. Finally, students and staff can enjoy secure extended wireless coverage with seamless roaming across the wireless network.

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 distributed campuses with a flexible, powerful and intuitive tool to globally manage SonicWALL appliances and security policy configurations 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

Internet access is increasingly central to learning. Compromised security threatens school programs and undermines budgets. By delivering powerful, granular and complete security for school networks without escalating infrastructure complexity or costs, SonicWALL provides an intelligent approach to leveraging limited budgets.