**EDUCATION**

**Helping Schools Secure Their Networks While Saving Their Budgets**

## Challenges and Opportunities

The challenges facing grade school educators are greater than ever before. The standards for academic achievement and the expectations of students' families continue to climb. At the same time, education budgets are tighter. Schools' technology infrastructures are caught in the middle, requiring K-12 IT administrators to literally do more with less.

Networked resources have addressed some qualitative issues. Online instruction materials and classroom management services supplement teachers' capabilities and free them from administrative chores. In addition, self-service portals and email communications increase the efficiency and effectiveness of administrative staff.

This reliance on the Internet brings new challenges. As the user population grows to include on- and off-campus students, faculty, administrators, contractors and parents, so do the threats to the network's security. This is further compounded by the ever-changing threat landscape. What K-12 IT administrators need is a network and information security solution that is effective, high-performing, flexible, and easy to manage. These are the types of solutions that only SonicWALL® delivers.

### Leveraging your connections

The use of networks to deliver instructional content cuts materials costs and improves the uniform availability of top-tier curricula. But many of these programs—like those utilizing video content—require unimpeded high-speed connections. When those connections are slowed by extraneous use, some of that value is lost. Increasing bandwidth just shifts the costs and sets the stage for more problems down the road.

Online administrative tools simplify implementation of district-wide programs and policies. They enable anytime/anywhere access to resources and communications for faculty, administrators and students. But the proliferation of mobile endpoints and the management of access levels can quickly turn into a nightmare. Since so much of this functionality is browser- and Internet-based, the traffic can seem like one giant stream. But blocking ports to address threats can seriously impact productive use of the systems.

> *"I consider SonicWALL to be one of the leading-edge providers of services like application intelligence and control. I am saving up to 15 hours a week with the reduction in support calls. That is human capital that my staff and I can put back into other projects."*
>
> **Ross Ellicott**
> **Manager of Network Operations**
> **Brick Township Public Schools**

A cornerstone of any campus network is its wireless connections. Originally adopted to avoid the costs and constraints of cabling, wireless access has become a lifeline to faculty members and their students. But wireless connections —intended to allow quick and easy access to the network— are vulnerable. Further, because access points are physically distributed, management can be difficult.

### The letters of the law

Overlaid on the security concerns of K-12 IT administrators is an extensive regime of regulations. Central to this is the Children's Internet Protection Act (CIPA), designed to protect minors from inappropriate content. Many states further regulate Internet access for students and the types of content made available. The private sector weighs in with concerns about the transfer of copyright-protected content and the liability this represents to schools.

Districts must take all reasonable steps to satisfy these regulations. More importantly, they must be able to demonstrate their compliance. This requires management tools that allow for deep visibility into network activity and detailed record-keeping.

### The budget handcuffs

For all the importance associated with K-12 IT security, districts do not have the financial resources to make it their first priority. This is not just a matter of buying new equipment or services. Any new equipment requires deployment and ongoing management.

## SonicWALL Solutions for K-12 Education

### Smarter security appliances protect networks and budgets

SonicWALL Next-Generation Firewalls (NGFWs) with patented[1] Reassembly-Free Deep Packet Inspection® deliver superior malware protection, intrusion prevention and application control. SonicWALL NGFWs scan every byte of every packet for the deepest level of protection. These award-winning security appliances can also be deployed as a NGFW combining content filtering, anti-virus, anti-spyware, intrusion prevention, anti-spam, application control and real-time visualization.

SonicWALL firewalls scan all flows, across all protocols and ports without file size limitations, meaning all inbound and outbound traffic is scanned every time. This is essential for modern attacks that can hide threats in the application layer. And SonicWALL NGFWs achieve this with industry-leading throughput for uncompromised network performance. SonicWALL's performance advantage assures schools get full value from their new, faster broadband connections that would be lost to a legacy firewall even just a few years old.

### More refined content filtering for easier compliance

Content filtering can be integrated into every SonicWALL firewall, eliminating the need to buy and maintain multiple stand-alone products. Unlike less sophisticated content filtering solutions, SonicWALL deep packet application layer filtering distinguishes good traffic from bad using a variety of industry-leading methods. SonicWALL Content Filtering Service (CFS) integrates "proxy avoidance" countermeasures to prevent students from circumventing associated controls

---

[1] U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

or engaging in unlawful activities. SonicWALL's enhanced reporting capabilities enable forensic analysis of all inspected traffic to simplify the regulatory audits.  As a contributor to the federal government's National Institute of Standards and Technology (NIST), SonicWALL is uniquely qualified to meet the requirements of CIPA and other relevant regulations

### Easy-to-manage remote access extends resource availability

SonicWALL Secure Remote Access (SRA) solutions speed and simplify connections between campuses, district headquarters, and home-based users. SonicWALL Clean VPN™ enables secure home study and 24/7 faculty and administrator access to school resources by encrypting all session traffic and stopping malware from entering the network. SonicWALL Smart Tunneling™ technology enables the segmentation of networks, prioritization of traffic, and layering of security managed by centrally-administered policies. The ease of configuration reduces the time and expense of implementations, while the browser-based management simplifies administration.

SonicWALL SRA provides secure access from every possible endpoint, regardless of OS, including mobile devices such as smartphones and tablets. SonicWALL Mobile Connect™, a single unified client app for iOS, provides Apple® iPad®, iPhone®, and iPod touch® users full network-level access to resources over encrypted SSL VPN connections.

### Clean wireless frees your network

SonicWALL SonicPoint™ secure wireless access points allow you to deploy seamless 802.11a/b/g/n wireless networks, protected by SonicWALL Clean Wireless™ technology and SonicWALL Application Intelligence and Control. SonicPoints are automatically provisioned and updated by the firewall for ease of management

and configuration. SonicWALL Clean Wireless defeats wireless intrusions, and decontaminates traffic of malware at the access point, enabling students to safely access school resources. SonicWALL Virtual Access Points (VAPs) create secure segmentation between trusted and un-trusted wireless users, so student traffic never bleeds into administrative sessions.

### Central management simplifies administration

SonicWALL Global Management System (GMS ®) provides a centralized policy-enforcement console enabling administrators to quickly, precisely and thoroughly create security policies, even accounting for contextual variables such as user and device identity, type of content involved, and time of day, week or month. SonicWALL Application Intelligence, Control and Visualization gives IT administrators granular control over network activity from a single point. This is essential for targeted policy enforcement and network resource management that will not impact productive activities and flows. Automatic updates of signatures for threats and applications are pushed to SonicWALL appliances to relieve school IT staff of that routine maintenance function.

SonicWALL Analyzer reporting delivers real-time analysis of network utilization to immediately identify and isolate performance issues. This level of detail is irreplaceable during operational and budget reviews. The browser-based dashboard simplifies help desk tasks and mitigates the impact they have on IT administrators' other responsibilities.

## SonicWALL Delivers Integrated, Cost-Effective Network Security Solutions

SonicWALL's family of Next-Generation Firewalls combines robust security services with high-speed deep packet inspection to provide small, mid-size and large academic environments with the best protection possible. SonicWALL appliances reduce cost, risk and complexity by integrating automated and dynamic security capabilities for comprehensive protection and maximum performance while enabling ease of deployment and management.

■ **SonicWALL SuperMassive E10000 Series**

The flagship of SonicWALL's Next-Generation Firewall platform, the SonicWALL SuperMassive™ E10000 Series is designed for large networks to deliver scalability, reliability, deep security and application control at multi-gigabit speeds.

■ **SonicWALL E-Class Network Security Appliance (NSA) Series**

Utilizing a high performance, multi-core architecture, the SonicWALL E-Class Network Security Appliance (NSA) Series provides Next-Generation Firewall protection and advanced application control and visualization for the most demanding networks.

■ **SonicWALL NSA Series**

With advanced routing, stateful high availability and high-speed VPN technology, the NSA Series provides security, reliability, functionality and productivity for geographically distributed campuses, central offices and large distributed environments, while minimizing cost and complexity.

■ **SonicWALL TZ Series**

SonicWALL TZ Series firewalls integrate gateway anti-virus, anti-spyware, intrusion prevention, content filtering, anti-spam and application control, offering high performance multi-layered network protection at a tremendous value for small organizations and branch offices.

■ **Clean Wireless Series**

SonicWALL Clean Wireless solutions combine high-performance 802.11n technology with our award-winning line of firewall appliances to deliver unparalleled wireless security and performance while drastically simplifying network set-up and management.

■ **SonicWALL Content Filtering Service (CFS)**

SonicWALL Content Filtering Service is ideal for school districts seeking a cost-effective, integrated filtering solution. This subscription-based service runs on all SonicWALL firewall appliances and leverages a dynamic database of millions of web sites, URLs and IP addresses.

## Scalable Integrated Solutions for Comprehensive Protection

SonicWALL complements its network security appliance line with a fully-scalable range of Secure Remote Access (SRA), Email Security, and Backup and Recovery solutions.

■ **SonicWALL Aventail E-Class Secure Remote Access Series and SRA Series for SMB platforms**

A variety of customizable features in SonicWALL's SSL VPN technology platforms ensure that both appliance series deliver the consistent, reliable access experience remote users want, and the control and ease of use administrators require. The robust E-Class SRA platform offers secure remote access to mission-critical applications and resources, an in-office remote access experience for end users, and unsurpassed levels of granular access control.

■ **SonicWALL Email Security**

SonicWALL Email Security solutions all deliver powerful protection against inbound spam, phishing, viruses, Denial-of-Service, Directory Harvest and Zombie attacks, while preventing outbound leaks of confidential information and violations of laws or regulations. Easy to use and manage, the self-running and self-updating email security solution is ideal for any size academic environment.

■ **SonicWALL Backup and Recovery**

The SonicWALL Continuous Data Protection Series offers small, remote and branch offices a flexible data backup and disaster recovery solution that automatically protects business assets from loss. Supporting Windows®, Linux® and Mac OS® through a single web GUI, it provides granular, globally enforced policy controls over the entire backup operation. Sophisticated file-set backup and agent-based de-duplication speeds backups and optimizes bandwidth, while maintaining data continuity and multiple revisions.

For more information on SonicWALL's solutions for education, please visit our web site at **www.sonicwall.com.**

> "I chose SonicWALL over Cisco due to the ease-of-use and manageability. It's also really easy to set up and get running on the network." Before, we had no idea where our bandwidth was going. Now, I can see how students consume hundreds of gigabytes of bandwidth a day on YouTube. We can save money through better bandwidth management."
>
> **Tom Gawczynski**
> **Network Administrator**
> **Crete-Monee School District**

**SonicWALL's line-up of dynamic security solutions**

NETWORK SECURITY · SECURE REMOTE ACCESS · WEB AND E-MAIL SECURITY · BACKUP AND RECOVERY · POLICY AND MANAGEMENT

**SonicWALL, Inc.**
2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600  F +1 408.745.9300
www.sonicwall.com

**SONICWALL®**
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™