SOLUTION BRIEF

Key Components for K-12 Cybersecurity

What to consider in selecting a security solution

ABSTRACT

This brief offers IT directors and administrators at K-12 schools and school districts an overview of deploying highly secure and cost-effective network security. It reviews core requirements, presents key components to consider when selecting a network security solution to meet those requirements, and examines how next-generation firewall (NGFW) technology from SonicWall delivers those key components.

Introduction

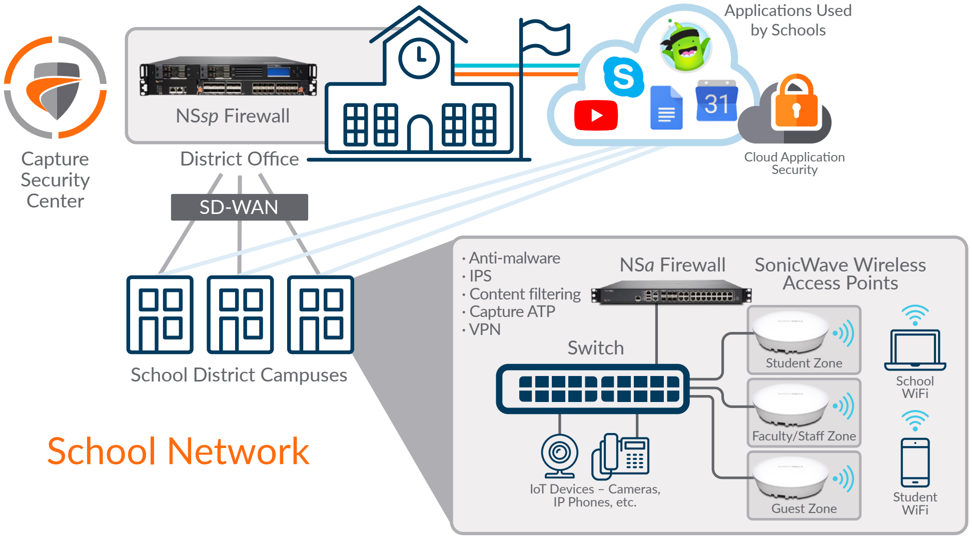
K-12 school districts share student, faculty and administrative data across local and wide area networks, wireless networks, cloud services and the internet. Districts must protect confidential and sensitive data from cyber-theft, protect students from inappropriate content, and secure the network from threats such as viruses, spyware and intrusions – all without impeding academic performance and productivity.

To maintain E-Rate discount eligibility, schools also must comply with the Children's Internet Protection Act (CIPA), by implementing a policy that protects minors from inappropriate web content. District directors of information security (IS) are tasked with selecting and procuring the most effective network security solutions within their budgets, while ensuring the greatest value and return on investment.

Core network security requirements for K-12

An effective K-12 network security solution must therefore:

- Protect students from harmful websites both at school and home on school-issued devices, in line with CIPA
- Comprehensively protect the network from threats
- Provide secure, high-speed wireless access for students, faculty, and staff using either school-issued or personal devices
- Optimize network bandwidth for academic applications to enhance performance and productivity
- Streamline deployment, management, and integration to lower total cost of ownership (TCO)



Key components to consider

To meet all these core requirements, several key components stand out for consideration when selecting a network security solution:

1. Gateway security services: These turn your firewall into a complete security solution that can prevent intrusions, block malware and spyware, inspect suspicious files, and provide application intelligence and control. Add SonicWall Advanced or Essential editions to get bundled security services. Or, choose from a host of services, such as Capture Advanced Threat Protection (ATP), Gateway Anti-Virus, Intrusion Prevention, Content Filtering Service and more.

2. Multi-engine sandboxing: This stops unknown, zero-day attacks such as ransomware at the gateway with automated remediation. SonicWall Capture ATP offers a cloud-based multi-engine sandbox analyzes suspicious code to help discover and block newly developed malware from entering your network.

3. Wireless network security: This key component extends the protection applied to your wired network to your WiFi networks, to provide secure, high-speed wireless access for students, faculty, and staff, whether using school-issued or personal devices. Our SonicWave 802.11ac Wave 2 access points (APs) can be untethered from the firewall, providing flexible management options. Take advantage of a broad range of advanced security features such as Capture Advanced Threat Protection (ATP) and Content Filtering Service (CFS) on the AP, a dedicated security radio for scanning, mesh networking capability to instantaneously expand networks, and single-pane-of-glass management with WiFi Cloud Manager (WCM) in SonicWall Capture Security Center (CSC).

4. DPI-SSL: Deep Packet Inspection (DPI) of encrypted Transport Layer Security (TLS) traffic ensures cyberattacks aren't evading security controls to infiltrate your network. Gain visibility and safeguard your network from encrypted threats with SonicWall Deep Packet Inspection of TLS, SSL and SSH (DPI-SSL), available as an add-on service on all SonicWall firewalls. DPI-SSL delivers deep protection against encrypted threats across a broad array of encryption protocols, and scalable SSL decryption and inspection performance without limitation.

5. Content filtering: This component offers a powerful protection and productivity solution to block access to harmful and unproductive web content from students, faculty and staff, in line with web content.

6. Unified Security Management: This component gives you more agility and capacity to govern the entire range of SonicWall security operations and services. SonicWall Network Security Manager (NSM) scales with your business and your security needs. From a single console, orchestrate all firewall operations, see hidden risks, discover misconfigured policies, and make compliance easier with a full audit trail. With a SonicWall NSM, centralize firewall management and gain more capability, not more complexity.

Deployment of key components in K-12 environment

A typical K-12 network might deploy a SonicWall NSsp firewall at the district, plus NSa or TZ firewalls at schools, each running gateway security services, including Capture ATP, and each securely connected via site-to-site VPN. Content Filtering Service aids in CIPA compliance. Use a TZ 370 or TZ 670 firewall to connect PoE-enabled devices without a PoE switch, including wireless access points, IP phones, cameras and more. SonicWave access points can be untethered from the firewall and managed via cloud. Cloud App Security protects productivity platforms such as G Suite in the cloud. Capture Security Center adds single-pane-of-glass governance of security, networking, cloud apps, and wireless operations and policies.

Conclusion

In summary, when evaluating a comprehensive network security solution, K-12 school districts should require the key components of content filtering, TLS inspection, gateway security services, wireless network security, and WAN acceleration, as well as global management over all. Content filtering protects students from harmful websites both at school and home on school-issued devices, in line with CIPA requirements. DPI-SSL enables the detection of increasing amounts of encrypted threats, while gateway security services prevent intrusions, block malware and spyware, and provide application intelligence and control, all needed to comprehensively protect the network from threats. Wireless network security extends that protection to provide secure, high-speed wireless access for students, faculty, and staff, using either school-issued or personal devices. In addition, WAN acceleration optimizes network bandwidth for academic applications to enhance performance and productivity, while an integrated global management system streamlines deployment, administration, and integration, to lower TCO.

Learn more at www.sonicwall.com/k-12.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com