# Next-Generation Firewalls and Content Filtering: A Guide to Selecting the Right Solution for K-12 Schools

## CONTENTS



SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

## Executive Summary

This paper discusses how Next-Generation Firewalls (NGFWs) address the security and content filtering challenges faced by today's K-12 organizations. NGFWs deliver a comprehensive and highly granular solution for network security, bandwidth management and content control that reduces the cost and complexity of running educational networks. This paper also provides a competitive analysis of leading NGFWs and Content Filtering solutions from Cisco, Fortinet, Juniper, Lightspeed, SonicWALL and Websense.

# Introduction

If you are an IT professional at K-12 schools, you are faced with a growing list of educational and administrative demands on your network. Do any of the following issues sound familiar?

- E-learning, 21st-century classroom, and anytime/anywhere learning initiatives have pushed your existing network security solution to its limits.
- Your existing network security solution requires a collection of "helper" products to deliver adequate threat protection and other essential security capabilities, driving up costs and management complexity.
- Your existing content filtering solution is too costly.
- Inadequate network capacity and performance are resulting in high latency and a negative user experience for students and staff.
- Web 2.0, collaboration, and multi-media apps are causing bandwidth usage and associated costs to grow out of control
- Your network security solution is incapable of identifying and providing granular control over the specific apps and users consuming network resources.
- You are stuck with "one-size-fits-all" access rules that either constrain access or do not protect resources well enough.
- You are unable to de-prioritize less important traffic in favor of mission critical or time-sensitive apps.

# The Impact of Ongoing Trends and Key Initiatives

IT environments for K-12 organizations are characterized by a number of issues, initiatives, and over-arching trends. Chief among these is a growing culture of openness. Once exclusive to the higher education segment, the philosophy that "good learning" is fostered by students being able to freely and thoroughly explore their ideas is now working its way into the K-12 arena. For IT, the result is the need to provide comprehensive protection against the risks that such openness introduces, and to have this protection be as unobtrusive as possible.

Other trends and challenges re-shaping the requirements of an effective K-12 security and networking solution include the following.

**The 21st century classroom**
Initiatives that support engaged learning and deliver increasingly individualized curricula are necessitating broader access to applications and technologies that facilitate better, more modern teaching and learning methods. This is driving greater network access and Internet usage –not only by students and faculty, but also by parents as they leverage online resources to monitor their children's progress and participate in the education process. Greater protection is required as more users, applications, and resources are exposed to more threats than ever before.

**Budget constraints and manpower limitations**
Being under-funded is status quo for the majority of school districts, and current economic conditions only make matters worse. Today's K-12 educators are stuck trying to deliver a 21st century classroom on a 20th century budget. Individual teachers are also being called on to supplement understaffed IT departments by taking an active role in network and system administration. Cost-effectiveness is a critical requirement for K-12 security and networking solutions, but so too are efficiency and ease of management

**Compliance and data privacy**
Preserving federal subsidies for Internet connectivity and related technologies requires compliance with the Children's Internet Protection Act (CIPA). In practice, this requires far more than a basic URL/content filtering solution. K-12 organizations need the ability to monitor and control the activities of individual users on a broader basis – not just for web traffic. They also need to successfully combat proxy sites (which can be used to bypass many filtering products) and to enforce policies on a granular basis (versus having their users be constrained by "one-size-does-not-fit-all" access rules).

**Network/Internet bandwidth explosion**
Initially sparked by government subsidies, the recent explosion of network and Internet bandwidth is now fueled by other initiatives. Many school districts are embracing Software as a Service (SaaS) offerings, an approach that allows them to quickly and cost effectively expand their app portfolio without the need for substantial in-house investments. Bandwidth-hungry apps such as LifeSize and other video conferencing solutions are also being used to enable remote/collaborative teaching – or simply to cut travel costs by more efficiently supporting school board meetings. In addition, there is an extensive set of popular e-learning applications (e.g., Mathletics.com, Moodle.org, and Scholastic Read 180), the rising prevalence of online standardized testing, and the use of other online services for summer school and credit recovery programs. The resulting growth in bandwidth usage dictates the need for:

- High performance, high capacity network security solutions;
- Better bandwidth visibility, to help rein in costs by minimizing unwanted application traffic; and,
- Better bandwidth and application control, to help manage contention and ensure a positive user experience, particularly for mission critical (e.g., online testing) and latency-sensitive apps (e.g., VoIP and multi-media collaboration).

**Anytime/anywhere learning**
A sub-component of the 21st century classroom, anytime/anywhere learning provides the opportunity for students to learn at their desks, and, ideally, wherever they are located at whatever time they choose. A related issue is the growing need to support network access from a broad range of devices, including ones that are not owned or controlled by the school's IT department. This helps with anytime/anywhere learning, and provides an attractive alternative to historical 1:1 initiatives that can dramatically reduce a school's laptop-related expenditures. Now more than ever, it is necessary to securely enable remote access to educational and administrative resources, and protect these resources from compromised client devices.

**Widespread WLAN usage**
In addition to not aligning well with the concept of anytime/anywhere learning, providing fixed network access for all students and staff can be challenging from a physical facilities and cost perspective. This is

why Wireless LAN (WLAN) technology is now common even for K-12 institutions. WLANs, however, bring with them the need to protect against the risks of a networking technology that is often purposefully configured to be relatively permissive and often extends beyond the physical boundaries of the facilities.

## Strengths and Benefits of the SonicWALL Approach

Ongoing trends and initiatives have not changed the requirements for effective security and networking solutions. The legacy products and technologies most organizations continue to rely on have failed to keep pace with these changes.

Consider the traditional stateful inspection firewall. It is unable to reliably distinguish individual applications. Neither can it provide sufficient visibility into how network resources are being consumed, nor enable granular control over users and apps. Attempts to correct these deficiencies have proven incomplete. They also have a negative impact on latency and throughput.

A similar situation persists for commonly deployed web proxy/filtering products. The accuracy, visibility, and granularity of control delivered are simply not sufficient for today's K-12 needs. And it is certainly not commensurate with the annual subscription costs typically incurred!

In both cases – firewall and web filter/proxy – the scope of capabilities provided is insufficient. The result is already over-taxed IT departments must purchase and maintain more point products to fully meet their needs (e.g., for comprehensive threat protection, secure remote access, and WLAN security).

**The SonicWALL solution for K-12 organizations**
In contrast to the legacy technologies and approaches commonly in use today, SonicWALL® provides K-12 schools and districts of all sizes with next-generation security and networking solutions ideally aligned with emerging requirements. In particular, with the SonicWALL family of Next-Generation Firewalls (NGFWs), K-12 organizations obtain:

- The ability to accurately identify all applications and users on the school's network
- Numerous tools for efficiently visualizing and controlling precisely how network bandwidth is consumed
- Advanced firewalling and web/content filtering capabilities, *plus* an extensive set of essential countermeasures and networking capabilities in a single, consolidated device
- A platform architecture that supports simultaneous operation of all capabilities while introducing minimal latency and delivering maximum throughput

The result is an extremely powerful network security and bandwidth control solution that is easy to implement, operate, manage, and maintain – and is also remarkably cost-effective. It is not uncommon for schools to obtain the fully equipped SonicWALL NGFWs they require for less than they are paying to renew their existing web/URL filtering subscriptions. For example, due to per user licensing, Websense alone can cost three times as much as a central site NGFW from SonicWALL, of which content filtering is just one capability. And those schools that implement Websense still have to pay the costs of a stateful packet inspection firewall, intrusion prevention service and packet shaper.

## Providing Unmatched Visibility and Control

The first of three core technical elements responsible for the strengths and benefits of the SonicWALL NGFW is SonicWALL Application Intelligence, Control, and Visualization (AICV). The key to delivering truly effective network security, AICV is what enables K-12 organizations to support a culture of openness yet still provide comprehensive protection. With AICV, schools can control who has access to which specific

resources (e.g., apps and individual app functions) under which specific conditions (e.g., time of day, status of client device), and even to what extent (e.g., in terms of bandwidth allotment).

**Application intelligence**
SonicWALL AICV leverages SonicWALL's Reassembly-Free Deep Packet Inspection (RFDPI) and an extensive application signature database to scan every packet – across every protocol, port, and physical interface – to identify and control over 3,500 applications and individual application functions. Unlike traditional stateful inspection-based firewalls (which depend on unreliable methods for classifying network traffic), SonicWALL AICV has no dependence or limitation relative to the ports and protocols being used or the direction of traffic flow. It can optionally be extended to SSL encrypted sessions as well. New signatures are constantly being generated and are automatically delivered and implemented without administrators having to update rules or underlying application objects. Custom signatures can also be created to extend support to any homegrown or uncommon applications a school may be operating, as well as to individual elements of personal or otherwise sensitive information (for data privacy purposes).

**Application visualization**
Application visualization enables K-12 IT staff to see what is happening on their networks – which specific applications are being used, by which users, when, and to what extent. Such information is essential for policy and rule development, efficient troubleshooting and analysis, demonstrating accountability and compliance, and exposing wasteful or unwarranted consumption of bandwidth.

SonicWALL provides extensive, on-box visualization and analysis tools. The SonicWALL Visualization Dashboard includes the Real-Time Monitor (for viewing summary and system-level information) and the App Flow Monitor (for viewing granular, real-time data pertaining to applications, users, URLs, initiators, responders, threats, VoIP, VPN, devices, and content). Available data can be viewed in multiple formats (e.g., list, pie chart, and graph), subjected to virtually any series of filters, and manipulated in countless ways to maximize its usefulness.

The SonicWALL solution also supports NetFlow/IPFIX with Extensions, an open, industry-standard mechanism. All the same in-depth, application-oriented Dashboard data can be exported to external collectors and tools (e.g., SonicWALL Scrutinizer).

**Application control**
Application control is the actual enforcement of security policies via the execution of responses to network traffic. This is the end-goal of application intelligence and visibility. With SonicWALL AICV, K-12 IT staff can configure highly flexible policies based on application type, individual application, or specific application functionality (e.g., file transfer within IM), while also accounting for a wide range of contextual variables, including user and device identity, the type of content involved, and time of day, week or month. The SonicWALL solution supports numerous actions – not just allow, block, and log – to manage bandwidth prioritization and limits. Administrators can even create macro-objects consisting of groups of applications, URLs, or URL categories, and then apply bandwidth management rules to those objects. Unlike competing products, applications and URLs need not be managed as separate entities with separate GUIs.

## Architected for Performance and Affordability

The underlying architecture of the SonicWALL Reassembly-Free Deep Packet Inspection® (RFDPI) is a highly efficient, single-pass engine designed specifically for real-time applications and latency sensitive traffic. RFDPI delivers control and protection without proxy connections, handoffs to separate modules, or costly packet processing and stream-reassembly routines. Coupled with a range of purpose-built, multi-core hardware platforms, the result is superior performance and price/performance, even with the extensive feature set SonicWALL NGFWs support and the numerous layer-7 inspections they perform.

# Delivering Consolidation, Ease of Management, and Lower TCO

With the SonicWALL NGFW, K-12 organizations obtain much more than a highly effective firewall. Full-featured web/content filtering, advanced threat protection, secure remote access capabilities and more are all included as integral components. With a robust, centralized management system, the result is a consolidated solution that substantially reduces total cost of ownership (TCO) by eliminating the need for numerous point products and vastly simplifying both initial deployment and ongoing administration.

**Effective web and content filtering for Less**
The SonicWALL Content Filtering Service (CFS) combines a local cache of URL ratings (for high performance) with a centrally maintained, cloud-based ratings database (for comprehensive coverage and timely updates). Support for Active Directory user/group information, a combination of local and district-wide policies, customized allow/forbid lists (i.e., exceptions), and 64 ratings categories enables granular policy enforcement. A specific "hacking and proxy avoidance" category helps put an end to students circumventing associated controls or engaging in unlawful activities. A combination of customizable, real-time and historical reports is available to monitor student activities and demonstrate CIPA compliance. Most importantly, with SonicWALL CFS, K-12 organizations obtain an enterprise-class content filtering solution without the need to purchase, implement, and maintain separate, dedicated content filtering devices and yet another management application.

**Comprehensive threat prevention**
SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service tightly integrate with the rest of the solution. These capabilities ensure allowed sessions are free from embedded threats such as malware and other types of attacks –without the need for separate devices and management tools. Unlike competing products, the SonicWALL RFDPI engine can scan both arbitrarily large files (i.e., there is no size limitation) and large numbers of small files for all types of malware, all while introducing negligible latency. Threat scans are bi-directional, enabling detection when threats "phone home," and are applicable for all protocols and applications regardless of port. SonicWALL supplements onboard signature language with an Intelligent Cloud Malware Detection Engine. Flows susceptible to malware infections are tokenized by the RFDPI engine and then compared in real-time – much like a high-speed DNS query – to a cloud database containing millions of additional signatures.

**Completely secure remote access**
SonicWALL Clean VPN is a powerful and innovative approach that addresses the user mobility and device proliferation associated with anytime/anywhere learning. With SonicWALL Clean VPN, a first "wave" of protection is provided by requiring user authentication, confirming that associated client devices comply with corporate policies/configuration standards, encrypting all session traffic, and establishing granular control over which applications and resources users can access in any given scenario. Integral malware scanning and intrusion prevention capabilities scrub all authorized sessions for embedded threats, thereby delivering yet another layer of protection.

**Completely secure WLANs**
Clean Wireless is SonicWALL's answer to many of the security, performance and management challenges that plague WLAN technology. By integrating SonicPoint-N Dual-Band access points with SonicWALL NGFWs, Clean Wireless allows K-12 administrators to consistently enforce one set of policies over both wired and wireless networks. All WLAN traffic is protected by the authentication and encryption mechanisms common to most WLAN solutions. It is also subjected to the granular access and bandwidth control policies enabled by SonicWALL AICV, and then scrubbed for all types of threats by the NGFW's other gateway security services. As an added benefit, centralized configuration and management of access points by SonicWALL NGFWs eliminates the need for separate, standalone wireless access controllers. SonicWALL NGFWs can also function as a secure wireless switch and controller that automatically detects and configures SonicPoint wireless access point devices.

**Simplified management and reporting**
SonicWALL Global Management System (GMS®) is a scalable and highly intuitive solution that helps K-12 organizations reduce TCO and ensure consistent, effective enforcement of network security policies. With GMS, administrators can efficiently manage NGFW configurations and view real-time monitoring metrics across distributed sites. SonicWALL Analyzer is a complementary web-based tool that further simplifies troubleshooting, bandwidth management, forensic, and compliance tasks by delivering fully customizable reports and dashboards illustrating and documenting all aspects of network activity – including which specific users are using which applications or sites, when, and to what extent.

**Complete, consolidated coverage**
The SonicWALL NGFW product line extends from the TZ 210 (supporting up to 110 Mbps of application-layer inspection and intrusion prevention) to the 5-model Network Security Appliance (NSA) Series (up to 1.4 Gbps), the 4-model E-Class NSA Series (up to 3.7 Gbps), and the 4-model SuperMassive E10000 Series (up to 30+ Gbps). The core feature set is consistent across models, including full AICV, IPS, and malware prevention capabilities. With this line of solutions, SonicWALL is able to meet the price, performance, and functionality requirements of any K-12 organization, from the smallest individual school to the largest district.

## Competing "Solutions" Fail to Make the Grade

Competing products typically fall short of SonicWALL NGFWs. Limitations of these competitors include:

- Inherently flawed app identification and control, because they rely on ports and protocols for initial classification and/or are unable to account for evasive techniques (e.g., use of non-standard ports, port hopping, protocol tunneling, and SSL encryption)
- Insufficiently granular policy enforcement, either in terms of who and what (i.e., apps/functions) can be controlled, or the variety of responses available
- Reliance on proxy-based technology, which negatively impacts performance and often leads to malware scanning limitations (e.g., in terms of file size or count)
- Malware scanning capabilities that are limited to a small subset of protocols
- Content filtering capabilities limited to a handful of protocols (e.g., ftp and web only)
- Multiple separate devices required to support a comparable set of security functions
- Dependency on third-party security components, which translates into sub-optimal performance, effectiveness and manageability
- Limited choice of hardware platforms and/or inconsistency in terms of which capabilities are available on which platforms
- Non-integrated wireless access point devices must be individually and manually configured

Table 1 further illustrates many of the advantages of the SonicWALL NGFW by providing a side-by-side comparison with several other "solutions" currently in use or being considered by many K-12 organizations

| Capabilities | Firewalls/NGFW Products | | | | Content Filtering Products | |
|---|---|---|---|---|---|---|
| | SonicWALL E-Class NSA, NSA and TZ | Cisco ASA Series | Fortinet Fortigate | Juniper SRX Series | Lightspeed Systems Suite | Websense WSG |
| **App Intelligence** | 3500+ signatures | < Signatures | < Signatures | < Signatures | Not supported | Supported |
| | Highly accurate and effective | Inherently flawed | Supported | Inherently flawed | Not supported | Supported |
| | Support for custom signatures | Not supported | Not supported | Not supported | Not supported | Supported |
| **App Visualization** | Comprehensive on-box monitors | Not supported | Not supported | Not supported | Not supported | Not supported |
| | Export detailed app-oriented data | Not supported | Not supported | Not supported | Not supported | Not supported |
| **App control** | Numerous response options | Limited | Supported | Supported | Not supported | Supported |
| **Bandwidth management** | Highly granular enforcement | Less granular | Less granular | Less granular | Not supported | Supported |
| | Highly granular enforcement | Not supported | Supported | Supported | Only based on port or content category | Supported |
| **Content/URL filtering** | Extensive signatures | Not supported | Supported | Supported | Supported | Supported |
| | Highly granular enforcement | Not supported | Supported | Supported | Supported | Supported |
| | Easy exception handling | Not supported | Supported | Supported | Supported | Supported |
| | Blocks proxy sites | Not Supported | Supported | Supported | Supported | Supported |
| **Breadth of security functions** | Extensive (FW, SSL VPN, IPsec VPN, IPS, AV, Anti-spyware, URL filtering, Etc.) | Can't run all capabilities simultaneously | Extensive | Limited | Not supported | Web security and DLP only |
| **Anti-Virus and Anti-Malware** | No file size or file count limitations | Only with add-on module | Limited file sizes | Not supported | Supported | Supported |
| | Scans all traffic on all ports, protocols, interfaces | Only with add-on module | Supported | Not supported | Supported | Supported |
| | Cloud augmentation | Not supported | Not supported | Not supported | Not supported | Supported |
| **Performance** | Single-pass inspection engine | Not supported | Supported | Not supported | Not applicable | Not applicable |
| | No proxies | Supported | Supported | Not supported | Not applicable | Not applicable |
| | Multi-core hardware | Not supported | Asic-based | Multi-core hardware | Not applicable | Not applicable |
| **Price/performance** | Excellent | Poor | Fair | Poor | Fair | Poor |
| **Platform selection** | 14 models from 100mbps-30gbps for NGFW functionality | 11 models from 75mbps-10gbps | 19+ models from 10mbps-60gbps | 10 models from 65mbps-30gbps | 2 models from 45mbps-10gbps | 2 models |
| | Consistent feature across all platforms set | Not supported | Supported | Not Supported | Supported | Supported |
| **Technology ownership** | 100% In-house for security | In-house | In-house | In-house | In-house | In-house |
| **Manageability** | Centralized control, highly intuitive, and includes numerous efficiency features | Centralized | Centralized | Centralized | Centralized | Centralized |

**SonicWALL Application Intelligence, Control and Visualization**

SonicWALL Application Intelligence and Control can maintain granular control over applications, prioritize or throttle bandwidth, and manage website access. Its comprehensive policy capabilities include restricting

transfer of specific files and documents, blocking email attachments using user-configurable criteria,

customizing application control, and denying internal and external web access based on various user-configurable options.

- The SonicWALL App Flow Monitor provides real-time graphs of applications, ingress and egress bandwidth, active website connections and user activity.
- This visualization capability enables administrators to effectively monitor all the traffic and users, and take action to revise policy based on critical observations.

**SonicWALL Global Management System**

The SonicWALL Global Management System (GMS) provides school districts with a powerful and intuitive solution to centrally manage and rapidly deploy SonicWALL firewall, anti-spam, backup and recovery, and secure remote access solutions in distributed environments.

- Flexible deployment options include software, hardware or as a virtual appliance.
- SonicWALL GMS also provides centralized real-time monitoring, and comprehensive policy and compliance reporting.
- GMS streamlines security policy management and appliance deployment, minimizing administration overhead.
- For added redundancy and scalability, administrators can deploy GMS systems in a cluster configuration.
- The SonicWALL Application Traffic Analytics solution is a combination of a SonicWALL Next-Generation Firewall and one of the software tools in SonicWALL's suite of traffic flow analysis applications, including SonicWALL Global Management System (GMS) 7.0, SonicWALL Analyzer and SonicWALL Scrutinizer.
- The incorporation of next-generation syslog and IPFIX for application traffic analysis results in granular, flexible and easy-to-use real-time application level reporting capabilities.

**Off-net content filtering**

K-12 schools benefit from a solution that enforces school content filtering policy on mobile or remote devices regardless of whether they are connected (locally or by VPN) or disconnected from the network. Off-Net Content Filtering technology enables schools with remotely distributed or at-home students to maintain compliance with CIPA regulations.

# Conclusions

The bottom line is SonicWALL NGFWs are uniquely capable of addressing the network security, bandwidth management, and content control challenges currently facing today's K-12 organizations. Legacy firewall and web filtering products have failed to keep up with the changing requirements and industry-specific initiatives – such as developing a 21st century classroom and supporting anytime/anywhere learning. SonicWALL allows everyone from the smallest private school to the largest district to obtain a solution that:

- Provides unmatched visibility into how network/Internet resources are being used
- Restores full, granular control over network/Internet access and bandwidth consumption
- Supports widespread use of diverse e-learning, Web 2.0, multi-media collaboration, and SaaS applications by providing essential threat protection while eliminating performance bottlenecks and enabling priority treatment for important or time-sensitive traffic
- Simplifies and reduces the cost of achieving compliance with applicable security and data privacy regulations, such as CIPA
- Reduces network complexity, administrative effort, and TCO by consolidating essential network security and control capabilities in a single, high capacity, low-latency platform


SONICWALL®

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