SONICWALL® | the JOURNAL

EDUCATION LEADERS ON...

Supporting Safe and Effective Digital Learning

SONICWALL | the JOURNAL

INSIGHT SERIES: EDUCATION LEADERS ON...

What Are They Thinking?

Leadership Insights on Issues in Educational Technology

CONTRIBUTORS:

Matt Federoff, chief information officer, Vail School District, Arizona

Jessica Levene, learning technology specialist, Volusia County Schools, Florida

SUPPORTING SAFE AND EFFECTIVE DIGITAL LEARNING

The proliferation of mobile devices and the push toward collaborative learning in today's K-12 schools has presented new security challenges for district IT departments. How do schools and districts ensure the security of their infrastructure while fulfilling the needs of new learning initiatives? *THE Journal* spoke with two schools and security vendor SonicWALL to get their insight.

What does collaboration mean to today’s digital learner and why is it important?

MATT FEDEROFF: What we have called “school” has always been associated with a particular place and a particular time (i.e., “Our school is located a XYZ address, and we start on Monday at 8 am”). Further, a student (or teacher), who you could work with, was limited to whoever was in the building at any given moment—who was in your class, or a staff member who shared a planning period with you. So collaboration, if it happened at all, was limited to a particular time, place, and those people sharing that time and place with you.

With modern collaborative tools, such distinctions become irrelevant. We can “do school” whenever and wherever we happen to be, and with whomever shares our interests.

JESSICA LEVENE: Collaboration for today’s digital learner means more than being able to interact and work towards a common goal with someone in a face-to-face setting. Today, collaboration includes being able to communicate and contribute to a common task with individuals from all over the world using mixed modalities. With the ability to asynchronously work on a cloud document or use real-time chat features to create a web-based presentation, today’s learners must develop digital citizenship and communication skills. Working in groups to create original ideas and evaluate sources will enable learners to succeed in today’s technology-rich environment.

The importance of collaboration is expressed in many of our curriculum standards, including the International Society for Technology in Education (ISTE) NETS-S and Common Core Standards. These standards emphasize engagement in discussion with peers and creation of original works through a group process. Working together promotes critical thinking because students move beyond memorizing rote knowledge to become active learners who discuss, create, and solve authentic problems. With technology providing a multitude of opportunities to collaborate without the barrier of location, students become aware of diverse perspectives. The communication skills that students gain through working in groups will be invaluable as a 21st century digital citizen. When students enter the workforce, they will need both face-to-face and virtual collaborative skills to apply to collaborative projects and communication in the workplace. The importance of collaboration has implications for districts, schools, and teachers. Safe, monitored online collaborative areas for students can be used, such as blogs, wikis, and educational social networking sites. When students and teachers are provided with district-supported online tools, teachers can apply scaffolding to allow students to use these areas as opportunities to practice and develop their virtual collaborative skills.

shutterstock.com

TECHNOLOGY INSIGHT FROM SONICWALL: With the ever increasing volume of traffic driven by user collaboration—including large media file attachments and links to streaming content—throughput is now a major consideration in evaluating security equipment. The closer to line speed a security measure performs, the better. Some organizations seek to address the issue with increased bandwidth and an increased number of switches accessing the network, each with their attendant security measures and often load-balancing solutions in front of it all.

This can get expensive and complex. And any piece of equipment through which traffic passes can become a chokepoint. Underpowered processors or store-and-forward architectures in the appliances can introduce latency into the flow. When threats are detected, remediation can further slow traffic. Fewer, faster systems can assure better performance and lower costs.

What is the role of anytime, anywhere learning in K-12 education?

MATT FEDEROFF: Working in such a fashion, though, changes how we end up "doing school." The sort of assignments, the assessment, the transactions between individuals changes. The typical classroom teacher is often caught up in taking care of the "loudest and the least"...whereas in anytime, anywhere learning, anyone can participate and contribute. That's why I like to call it "anytime, anywhere, anyone" learning.

The tools change the medium of exchange between teacher and student in that we have much greater freedom of opportunity to engage in conversation and trade ideas. A teacher can solicit and define the quantity and quality of contributions, because every student can participate and in fact you can know that every student did participate. This is simply not possible in classic "classroom discussion" situations.

JESSICA LEVENE: I remember when "homework" was a dreaded word because it meant learning and completing schoolwork outside of the classroom. However, in today's digital world, the role of anytime, anywhere learning is essential in education. We live in an information-rich society where students are accustomed to using a mobile device from anywhere at any time to find information. Our 21st century digital students are constantly learning every time they Google a question or catch up on the latest news on Twitter. Although this is considered informal learning (and in some cases may not be the most reliable information), the underlying premise is that students are actively seeking information. This momentum can be applied to K-12 education because we can use a student's desire to access information and socialize by providing web-based digital content and tools accessible 24 hours a day, seven days a week. Many teachers, schools, and districts have already initiated this by creating online discussion areas, class websites, and web-based desktops where students have access to their course materials and a way to engage in social learning with their peers. With Web 2.0 tools and mobile devices, both students and teachers can create websites, update blogs, and create digital books to share with all students in the class for anytime learning. For example, a teacher sets up a collaborative wiki where students can post their latest e-book on a science topic. When the students come home from school, they access the wiki from their smartphone or tablet and they download all 21 of their peers' e-books on science and read them from cover-to-cover. This means that students not only have anywhere access, but they are exposed to the subject-area content multiple times. Now that students and teachers can create their own content and post to web-based services, students can truly have access to their classroom anytime and anywhere.

shutterstock.com

TECHNOLOGY INSIGHT FROM SONICWALL: Secure Remote Access (SRA) has moved from a small, precious component of the network for a core constituency to become the vast outer ring of the network serving many—if not all—users. Of course, users can fall into several different groups, each of which has its own needs and permissions. The smarter the remote access solution, the better the user experience and the easier it is to manage.

Trusted users can be expected to gain access via devices with client controls in place. Casual users cannot, especially with the proliferation of various endpoints like tablets and smart phones. Intelligent SRA can recognize the different levels of control required, prioritize traffic accordingly (including latency-sensitive streams like VoIP and video), and integrate with intelligent security appliances to enforce centrally managed policies.

What are the top three challenges for any district in implementing an effective, safe and secure 21st century learning environment?

MATT FEDEROFF: First, high quality wireless service that covers the entire site, and allows multiple wireless networks and authentication methods. Second, a robust authentication system that can be leveraged across all Web 2.0 tools to improve ease of use and prevent unauthorized use. Finally, a powerful but highly granular content filter that can make filtering decisions based upon user identity, machine identity, and subnet.

JESSICA LEVENE: First, increasing trends in education include Bring Your Own Technology (BYOT) and Web 2.0 tools that allow students to collaborate and publish. With BYOT, districts allow students to bring in their personal devices to be used as an instructional tool for learning.

Next, as districts begin to implement BYOT and other web-based learning environments, there are many concerns for how to provide students with a secure network so they are filtered from inappropriate content. At the same time, districts must ensure that the devices using the district's network are not bringing in viruses and other malware that could compromise the network's security and data. Some very important questions address challenges districts encounter when implementing a 21st century learning environment, including the following: Will students have individual accounts that they use to login to the network? How will bandwidth and other data be tracked so that if a problem occurs while students are working on an assignment, the district's IT department can identify and fix the problem without it hindering students' learning? How will user credentials, along with student, and staff data be protected, especially if students are connecting their own devices to the network? Will there be an open SSID that students use to connect their devices? A major challenge arises if student-owned devices in BYOT have viruses or do not have virus-scanners when they enter the network. Many schools and districts have started to integrate mobile devices, such as iPads, for use in the classroom. This presents another challenge which is to ensure that the mobile versions of websites are filtered the same as the full version of the website when using a district's network.

A final challenge and very important area to address is the Acceptable Use Policy (AUP). Technology is ever changing as Web 2.0 tools and mobile devices become a part of the 21st century learning environment, the AUP should be reviewed and updated each year to reflect and communicate this environment.

TECHNOLOGY INSIGHT FROM SONICWALL: The technical expression of how users are interacting with the network is on the application layer. The applications users are running are either permitted, or not. Inside the permitted group, some applications deserve higher priority than others. Next-Generation Firewalls supplying Application Intelligence, Control and Visualization (AICV) enable granular scanning and filtering for the most targeted and intelligent security possible. This improves the quality of threat detection—especially the new web-borne application layer threats—and minimizes the disruption when threats are detected. It also gives IT administrators application-level controls for policy enforcement and traffic prioritization.

These capabilities can, in effect, free bandwidth and allocate it where it is most needed. They can automatically implement policy and prioritize flows by application type and user. And they can provide the analytics necessary to fine tune the network moving forward.

What are the biggest mistakes you've seen a district make in securing their school networks for digital learning?

shutterstock.com

MATT FEDEROFF: Wireless that's either too locked down or too open. If it's too open, everyone can get in. But if you lock it down too much, and make no provision for visitors, then the password gets shared out and the security is lost.

A content filter set with only one filtering profile. This is frustrating for teachers and students, as you can't fine tune it to particular audiences. It's either too locked down, and teachers are frustrated or, after being frustrated, IT is pressured to open it up and kids are left unprotected.

JESSICA LEVENE: As districts continue exploring options for secure digital learning, one mistake would be in trying to establish a school network with a "one-size-fits-all" approach. It is important for networks to provide ALL users with filtered, age-appropriate content. By not having an option for granular access, the secure network will likely not address the needs of students and teachers. For example, a district may choose to use individual student accounts for authentication to the network. While the majority of students will have every "gaming" category blocked, there may be instances where a specific group of students and teachers need different access. As part of the curriculum for a "game design" course, students may need to explore and evaluate current games to develop knowledge they will apply for their course project. Without granular access, a district would not have the option to provide a specific group of students tiered access. Establishing a flexible, customizable network that remains secure and safe will avoid securing a school network that is too restrictive and not conducive to learning.

TECHNOLOGY INSIGHT FROM SONICWALL: Regardless of how the network is accessed—wirelessly, via a web portal, or directly (including Secure Remote Access)—even the most comprehensive Acceptable Use Policy must ultimately be enforced by a firewall. Aided by Application Intelligence & Control built into Next-Generation Firewalls, the right application controls are granular enough to enforce permissions by application, by user group (e.g., students vs. faculty), and even by individual users. This is also a more targeted way of implementing content filtering, simultaneously satisfying regulatory requirements and providing a better user learning experience. The permissions can be modulated from "full on" to "throttled" to "blocked"…even by time of day, or point of origin. What's more, this Application Intelligence—knowing who is using what applications—is an invaluable tool for addressing regulatory compliance audits and budget planning.

This enables an optimization between real, important security issues and the best user experience possible. It also relieves users and administrators from struggling with human behaviors and focuses network management where it is most practical: how the network and applications behave.

What's the best advice you would give a district about securing their networking infrastructure to ensure a safe and effective 21st century learning environment?

shutterstock.com

MATT FEDEROFF: Use IP subnets to break your network into meaningful sections. For example, put your teachers on one wireless network and your students on another one. Or assign a high school to one subnet, and the elementary to another. With this you can apply different wireless networks and filtering rules to each subnet, giving greater flexibility, and improving your user experience.

JESSICA LEVENE: Collaborate with all departments who will be using the learning environment. Although the network will be set up and maintained by the district's IT department, the development should not rely just on the IT department. Much of the 21st century learning environment is curriculum-based. It would be beneficial to have ongoing discussions between the IT department and the district's curriculum department, school leaders, and educational technology department. Through a collaborative effort, these departments can discuss what curriculum tools are needed for students and the IT department can carry out the development of these curriculum needs by developing the safe, secure digital learning platform.

TECHNOLOGY INSIGHT FROM SONICWALL: Network topologies informed by needs and usage patterns require segmentation by security needs as well. User subgroups exist at multiple physical locations around a district. Some campuses might have wireless access throughout, while others may be strictly hardwired. This can raise huge issues for network management and place burdensome demands on IT administrators' time.

The solution is to maximize the integration and intelligence of the security infrastructure to increase visibility across the entire district and to enable policy enforcement from a central point of control. Intelligent wireless access points can not only thwart unauthorized access, but recognize rogue access points plugged into the perimeter. Next-Generation Firewalls performing Application Intelligence, Control and Visualization can further manage access and permissions by user group and even time of day, regardless of their physical location. The intelligent devices can all be managed from a central web-based console that is accessible to IT from any computer at any time of day.

ABOUT SONICWALL

Guided by its vision of Dynamic Security for the Global Network, SonicWALL® develops advanced intelligent network security and data protection solutions that adapt as organizations evolve and as threats evolve. Trusted by small and large enterprises worldwide, SonicWALL solutions are designed to detect and control applications and protect networks from intrusions and malware attacks through award-winning hardware, software and virtual appliance-based solutions. SonicWALL offers a massively scalable architecture to address the rapid increase in bandwidth speeds and escalating volume, frequency and sophistication of Internet threats. Moreover, SonicWALL drives the cost and complexity out of building and running secure infrastructures, thus enabling greater productivity and IT efficiencies.

ABOUT T.H.E. JOURNAL

T.H.E. Journal is a comprehensive resource that consists of a magazine, website, newsletters, and online resources. Every tool informs and educates K-12 administrators, technologists, and educators on the latest strategies and best practices influencing the way technology integrates into the landscape of teaching and administration at schools and districts nationwide. Each *T.H.E. Journal* asset delivers news, trends, features, case studies and expert advice on vital topics like security, policy and advocacy, smart classrooms, mobile and wireless computing, funding, green technologies, distance learning, administrative and academic computing, plus much more. For more information, visit www.thejournal.com.

For more information, go to: www.sonicwall.com

Produced by T.H.E. Journal, a division of 1105 Media Education Group. Sponsored by SonicWALL. Copyright 2012.