sponsored by

SONICWALL®

tech spotlight: security

shutterstock.com

presented by Campus Technology

1105 MEDIA Education Group

TABLE OF CONTENTS

The Consumerization of IT: Pendulum or Wrecking Ball? 2

A New Frontier in Security 6

6 Keys to Identity Management 7

NETWORK SECURITY: Berry College Case Study 9

NETWORK SECURITY: Securing Information in Higher Education Organizations 11

NEXT-GENERATION FIREWALL: SUNY College at Old Westbury Case Study.....14

The Consumerization of IT: Pendulum or Wrecking Ball?

The proliferation of consumer technology on campuses has created new challenges for IT departments. Will the pendulum swing back toward centralized IT, or is consumerization knocking down the old ways forever? BY JENNIFER DEMSKI

Smartphones, affordable software, cloud computing, crowdsourcing, social media.... The burgeoning consumer-tech market is creating new challenges for higher education IT departments. As increased expectations of mobility and connectivity have students and faculty looking to consumer technology to meet their academic needs, IT must revamp operations and infrastructure to meet the demand, while keeping security risks and budgets in check.

Is the new consumer IT model here to stay? While some IT administrators hope that the pendulum will eventually swing back to centralized, institutionally controlled IT, experts warn that the drive toward consumerization will fundamentally change IT operations for good. CT spoke with Sheri Stahler, associate vice president for computer services at Temple University (PA); Ronald Danielson, vice provost for information services and CIO at Santa Clara University (CA); and Carol Smith, CIO of DePauw University (IN), to find out how their institutions are tackling the trend.

CAMPUS TECHNOLOGY: Do you see the consumerization of IT as something that needs to be contained and controlled, or as an inevitable evolution of the campus computing environment?

RONALD DANIELSON: We're far beyond the point where use of personally owned devices can be controlled. At SCU, we do try to contain it somewhat. For example, we require that staff accessing administrative systems from home do so from a university-owned computer, to minimize the chances of another user of that computer introducing malware.

CAROL SMITH: I see this as an evolution that we should embrace and that will provide many benefits, but how we take advantage of it will vary across the different areas of IT. Redirecting some of our focus to virtualized applications that students can run directly from their laptops, for example, has the potential to reduce the number of physical computer labs that we must maintain across campus. Understanding students' expectations about how they manage their schedules online, access their files and coursework, pay bills, or check their grades will shape the functionality that we build into our student information systems. By recognizing their needs and finding the most efficient ways to enable students to complete these types of "administrative"

activities using their personal, mobile devices, we can help give them more time to focus on their academic lives—which is the core reason why they are on our campuses in the first place.

SHERI STAHLER: There are definitely concerns regarding security, but this trend is going to lead to a lot of innovation. The knowledge is out there, and when people can tap into collective knowledge so easily, that in itself leads to innovation. I've already seen a tremendous amount of creativity in how faculty and students use consumer tools to support their academic work. Plus, when you embrace this trend, you also eliminate silos both between IT and the academic departments, and among the academic departments themselves. When you are crowdsourcing and researching applications that have been used successfully in one discipline to see how they could be used in yours, those silos break down.

CT:How do you ensure the security of your campus network in a tech environment where users rely on personal devices, social networking software, apps, and other possibly vulnerable consumer IT products?

DANIELSON: IT professionals understand we can't "ensure" the security of our networks. We can only try to make the occurrence of a security problem less likely. We're at a juncture between keeping our current (relatively restrictive) security policies and making a large part of our client population very unhappy. And I think we're going to resolve this by accepting the risk of somewhat less security to make it easier for clients to use newer technologies that help them learn and do scholarship more effectively. We've started talking to our risk management people about what we're willing to let go and what we absolutely have to retain.

STAHLER: But policies, really, are a big component of network security now. We're constantly making sure our policies are up-to-date. Sometimes they're reactive rather than proactive, but when it comes to the use of consumer devices on the campus network, you have to have policies in place. What university information can users store locally? Or what happens if a device is stolen—can you wipe out the device's hard drive? What happens if personal information or sensitive data is leaked?

SMITH: We have a number of measures in place: secure-password policies; a data-encrypted, web-enabled administrative system; secure campus wireless; wired network to all campus offices, classrooms, and student dorm rooms; a secure LAN for shared network storage with encrypted VPN for off-campus access. We also provide antivirus software to all students for their personal laptops. Finally, we work hard to educate our campus clients about healthy and safe computing habits, per-

Virtual Consumers

Talk to an IT administrator long enough, and the conversation is sure to touch on virtualization and the cloud. And it's no coincidence that virtualization in higher ed has grown apace with the consumerization of campus IT.

"The two trends absolutely go hand in hand," remarks Sheri Stahler, associate vice president for computer services at Temple University (PA). "With virtualization, our users who rely on mobile devices or personal tablets or laptops become truly untethered. They can choose the device that works best for them, and access whatever they need, whenever they need it, as long as they meet the security requirements for the network."

In the consumerized IT environment, virtualization allows campus IT to be more effective in supporting the student academic experience. By establishing a virtual computer lab that students can access from their personal devices, for example, IT can reduce the number of physical computer labs it needs to maintain — and redirect that money and energy toward other projects.

"If students access the virtual computer lab on their own devices," explains Carol Smith, CIO of DePauw University (IN), "we can refocus our funding and staff time on things like managing the specialized applications that students need for their coursework and ensuring that they always have access to solid, reliable tools — tools that they don't need to learn how to manage themselves!"

In fact, virtualization has the potential to level the playing field in the consumerized tech environment. "By creating a virtual desktop that students can access on their personal devices," says Ron Danielson, vice provost for information services and CIO at Santa Clara University (CA), "we can expose students to software that they might not otherwise be able to afford, and provide capabilities that students and faculty need but their consumer devices either don't offer or offer poorly."

Extending virtualization to include internal cloud services creates a secure infrastructure for researchers, students, and faculty looking to utilize consumer web 2.0 tools and web-based applications. Temple University set up its internal cloud to provide a variety of configurations to end users, depending on their needs, reports Stahler.

"Our users can be a member of a greater server where they have access to a number of applications, like the Microsoft Office apps," she explains, "or, if a researcher relies on his own software but needs a way to host a WordPress site internally, we can provide an infrastructure that assures him that his site is secure and backed up. Researchers are very protective of their data, and the internal cloud allows them to use consumer technology in a secure way."

haps most notably through our participation in National Cyber Security Awareness Month each October.

CT: What is the role of central IT in this new computing environment?

SMITH: The role of the central IT department is to provide a sound, stable working environment that aligns with the mission of the institution. I'm not sure that our role has really changed because of this new computing environment, but the details and the day-to-day certainly have and continue to evolve. The IT department has to be able to balance solidity with flexibility to be most successful.

At the same time, while the core role may not have changed, some of the guiding principles that shape decision-making definitely have. In particular, the IT department has shifted from being the central entity on campus that provides and manages (i.e., "controls") all things IT to one whose most powerful function is to act as a connector and an enabler.

STAHLER: The key is recognizing this trend and making sure guidelines are put in place for social media use, for personal data, and for any factor that could compromise university assets. Protecting data has to be a university-wide priority.

The walls around our department have become much more permeable. Rather than putting blinders on and pretending that departments aren't setting up their own web servers, creating their own learning management systems, or relying on social networking and mobile apps, we need to know what's going on so we can figure out how best to support it.

At Temple, for example, every department and every researcher felt they needed their own server in front of them. In reality, those servers weren't backed up regularly and they weren't secure. In response, we created an internal cloud, so now there's a better option that's backed up regularly and undergoes routine random security checks. We specifically provided a number of cloud computing arrangements to match a wide variety of needs. We were able to provide the end users with a solution that would pay off for them in the long run. It's really about making the users better choosers.

DANIELSON: I agree. IT needs to be aware of what devices students, faculty, and staff are using on campus, what they're using them for, and what apps and services they're using. Then we need to get our staff using some subset of those devices so we know what benefits and concerns we're dealing with. There's not a lot of time after something gets introduced for us to do that (we had the first iPad network connection failure the morning it was introduced), so we have to be pretty agile.

CT: What effect does the consumerization of IT have on the tech budget?

SMITH: While it's doubtful that the consumerization trend will reduce overall expenses, it will definitely shift how we spend our budgets over time. In the future, for example, we will likely spend less on computer lab hardware and refocus those investments in areas such as virtualization, security, and even off-site cloud services. One key shift that we have already made is our transition

Focusing on the Core

How does the trend toward consumerization affect IT strategic planning on campus? Carol Smith, CIO of DePauw University (IN), responds:

"We organize our work in the IT department around three main areas: maintaining the infrastructure, or what I call 'the stuff' (the network, devices, the ERP, desktop tools, etc.); supporting campus workflow such as learning, living, teaching, and administrative business processes (what people do with 'the stuff'); and creating points of connection between people and information. Using these broad organizers enables us to keep our focus on the core of what matters, while providing the flexibility to adapt to the changing landscape over time.

"Another thing to consider is the notion of 'core' versus 'critical' in deciding how to make IT investments. A critical system or service is one that the institution absolutely needs to have. If something doesn't make the 'critical' cut, then we probably don't even need to offer it and we set it aside. Once we know if something is critical, we determine whether it is core: If it is something that is unique or culturally specific to our institution — that only we can maintain — then it is core.

"This classification helps us decide how best to provide services. If a system or service is core, then we know that we need to maintain it. But if it is merely critical, then we should consider outsourced or cloud solutions, if they exist and are economically feasible.

"As an example, when evaluating new e-mail systems three years ago, we determined that, while having an institutionally branded e-mail account for each student was critical, hosting our own on-site system was not core. This shaped our decision to transition to Google Apps for Education. I could see this same method being useful in determining how or when to embrace particular 'consumeristic' IT elements that our clients bring to campus."

related reading
Blurring the Lines of Network Security
The consumerization of IT is blurring the lines of network security on campus. Learn how the University of Rhode Island is balancing network protection with a culture of openness.

from managing an on-site e-mail system to using Google Apps for Education [GAE]. As we were evaluating potential new e-mail systems, a big factor in our decision to adopt GAE was the fact that a large percentage of our students and faculty members were already familiar with Google e-mail through their own personal accounts.

DANIELSON: On our campus it's too soon to be able to say what the financial impact will be. There's the age-old hope that when everyone has mobile devices we won't need computer labs, but I currently see students sitting in our labs using our computers with their laptop open on the desk beside them, so I'm not counting on that.

I think it is clear that the wireless network now becomes much more important, and needs to be much more robust and able to handle many more clients pushing increasing volumes of data, and I suspect that will lead to a decline in the number of wired ports on campus over time. We put one wired port per two seats in the library that we opened over three years ago, and I wouldn't put any in at client seating if we were doing it today. Also, many of the services that people are accessing with these consumer devices are off campus, so the need for commodity internet capacity will go up faster than it otherwise would have.

CT: What is your best piece of advice for campus tech administrators who are facing this challenge?

STAHLER: I was speaking at a conference on this topic recently, and I asked the audience—all higher ed IT people—how many of them think consumerization is just the pendulum swinging, as it does every couple of years, away from centralized IT, and that it would swing back toward centralized IT again. The majority of the people raised their hands. Wow...if you think that, you're going to be scrambling to catch up. I don't think we'll ever return to centralized IT. The network is going to be secure and centralized, but the devices? No. This "pendulum" is a wrecking ball. We need to adapt to it.

SMITH: And we need to listen. As campus technology administrators, we must balance what's important to keep the infrastructure reliable and secure with how much we let people do in order to accomplish their goals. To do that best, we must listen carefully to our constituents—in ways ranging from formal assessment to engagement with campus committees and informal dialogue with individuals across campus—so we can best gauge their needs. Then we can connect what we know about our own faculty and students with information from our external peers/colleagues and other larger studies in the field, to help us to understand where to focus resources.

DANIELSON: Study Zen. Consumerization is here now and will only increase in the future. There'll be some rough experiences, but we'll figure out a balance that's acceptable to everyone involved, and then we can move to the next crisis.

About the Author

Jennifer Demski *is a freelance writer in Brooklyn, NY.*

The Consumerization Gap

Do you know how many of your university's employees are using their personal smartphones for work purposes? In a 2011 IDC survey (sponsored by Unisys) of more than 3,000 workers and IT administrators in nine countries, only 34 percent of IT administrators reported that their organization's employees use personal smartphones to conduct business activities. In contrast, 63 percent of employee respondents reported using their personal smartphones for business purposes.

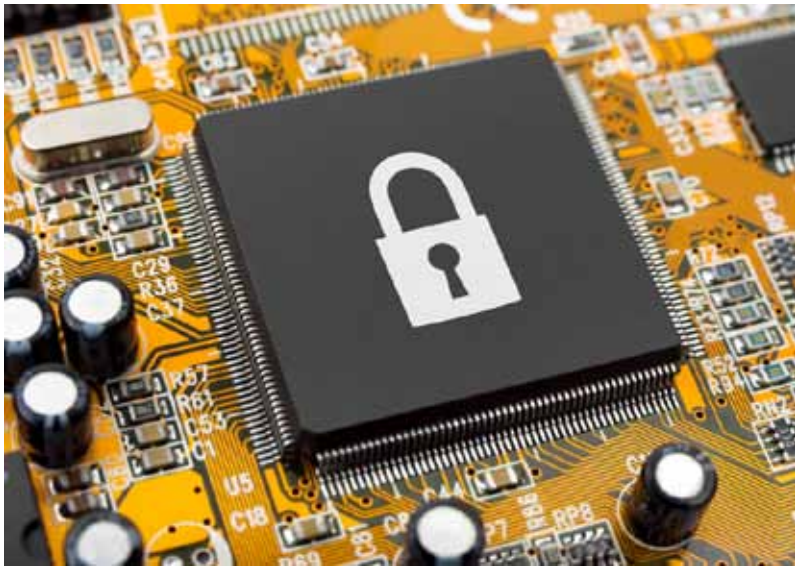
Similarly, while 13 percent of employee respondents reported using a tablet device for work, only 6 percent of IT respondents were aware of the tablet use.

In addition to highlighting the lack of awareness, the survey found a lag in technology adoption among IT organizations. When asked to rate their adoption and use of social networking applications and consumer devices for business purposes, 48 percent of responding IT workers considered their organizations to be "late adopters," while more than 60 percent of employee respondents considered themselves average-to-early adopters.

What's holding IT back? Among IT workers surveyed, the greatest barrier to enabling employees to use their own PCs and devices at work was security concerns, followed by the risk of viruses from social networks and challenges in developing corporate policies to support consumerization.

A New Frontier in Security

IT's job is to find security strategies that enable mobile and social apps. BY MARY GRUSH



shutterstock.com

For more than a quarter-million students each year at the Los Angeles Community College District, mobile devices and social software are critical tools for success. That's because these are often students' best and sometimes only ways to connect with peers, instructors, and education resources. In a recent interview, CT asked LACCD CIO Jorge Mata to discuss how institutions need to adapt their security strategies to encompass—and embrace—these tools.

Campus Technology: What is the impact of social software and mobile technology at LACCD?

JORGE MATA: Social media and mobility represent incredible promise at LACCD and in higher education in general. It is about going where the students are: The customers are there, and that's where you want to have your message. You want to join the dialogue, because the big conversation that uses these tools is going on 24/7, and it's going in every direction.

CT: What are the usual expectations about security relating to mobile and social media?

MATA: I think there is a tendency on the part of some administrators, once issues of security are brought up, to try to stop the conversation—it's often the first reaction. But as I always tell my boss, "If you only want me to tell you to *stop*, you are paying me way too much." IT departments and professionals should be in the business of *how*: How do we leverage social software and mobility? How do we make it safe? How do we allow the right things to happen?

A lot of older security technology has been very black and white—either "yes, you can do it," or "no, you can't." But the amount of content is so overwhelming now, that the minute you say no to one thing, you create a detrimental effect on another. For example, your institution may have a course on social media that actually teaches and requires the use of social software tools that you might have blocked in another context. You can't take a draconian approach in higher education. To me, blocking is a manifestation of failure—a sign that I've not been able to do my job. Again, I'm really in the business of *how*, and that's where I should put my efforts.

CT: Are social software and mobility dramatically changing the way you approach security?

MATA: Absolutely. In the past, user interactions were siloed, as in one person talking with a particular application. With newer, mobile technology and social media, you are suddenly looking at thousands of conversations that are happening simultaneously. This is overwhelming to traditional security, to legacy tools. We need to use security tools that are appropriate for this new environment, tools that will let you find that one element within thousands of concurrent sessions that may be an attack—find it and then surgically remove it.

That's what's new in security strategy: technology and security professionals looking more at the behavior and dynamic nature of interactions. This is not something that we did in the past. If you have chosen to stick to your traditional tools, you are already in trouble. Instead, you now need to use leading-edge security technologies—tools that can be driven by policy, that recognize identity, that work with mobile and social applications and their subcomponents in ways that let you apply business rules. You can't just block applications anymore. Applications tied to a specific port that you can turn off are a thing of the past. You have to understand how to enable applications safely. We will all be going in that direction. It's just a matter of time.

About the Author
Mary Grush *is Editor and Conference Program Director, Campus Technology.*

6 Keys to Identity Management

These best practices will help make your IAM project a long-term success.

BY IDAN SHOHAM

An identity and access management (IAM) project on campus can feel like a Sisyphean task: Just when access rights have finally been sorted out, the semester ends—and users change roles, leave campus, or require new processes.

Indeed, a number of IAM challenges confront the higher ed sector:

Mass onboarding (i.e., setting up access rights for new users) and deactivation at the beginning and end of each semester.

Different classes of users: Students, faculty, staff, alumni, and visiting scholars often have diverse technical requirements and business processes.

Widespread use of federation (infrastructure that allows an application to trust an assertion made in another administrative domain about the identity and access rights of a user) to enable cross-institution sign-on.

Relatively small budgets compared with those found in the business world.

Very large user populations. Alumni, in particular, can pose challenges because there are more of them every year.

On top of these issues, IT departments face a constantly changing technical landscape: integrating new applications and retiring old ones, complying with privacy rules, and dealing with vendor churn. For instance, Oracle's acquisition of Sun Microsystems will undoubtedly have far-reaching technical and financial implications for many institutions, and the impact of Novell's recent acquisition by Attachmate has yet to be felt.

The following best practices can help overcome such challenges and turn the seemingly endless IAM labor into an IT triumph.

DRIVER	METRIC	MEASURED AS
C	Password-reset call volume	Number of calls per month (average and peak) to the help desk to reset passwords
C	Help desk FTEs	Number of full-time equivalent staff required to support peak password-reset call volumes
C, P	Setup time	Number of IT work hours required to set up a new user
S	Deactivation time	Lag time between notification and deactivation of a departed user
C, S	Deactivation effort	Number of IT work hours required to terminate access for a departed user
S	Weak passwords	Number of systems that do not enforce length, character set, history, and dictionary rules
S	Standard caller authentication	Number of questions asked to authenticate help desk callers
C, S	Orphan accounts	Per system: number of user objects minus the number of legitimate users
C, S	Dormant accounts	Per system: number of accounts inactive for a certain number of days
C, S	Unassociated systems	Number of systems whose unique user identifiers are not mapped to a campuswide identifier
S	Admin password change interval	Per system: frequency of change of administrator passwords (in days)
C, P	Complexity of identity-change request	Number of different forms used to request changes to user identity data (name, phone, address, department, location, etc.)
C, P	Passwords per user	Average number of passwords a user must remember for institution-owned systems
C, P	Login prompts per user per day	Average number of times per day that a user must sign into an institution-owned system

Key: C = Cost reduction; P = User productivity; S = Security

FIGURE A

1) Don't Think of It as a Project

Identity and access management is the glue between the business processes that govern user access and the systems that users need to sign into. And since both business processes and systems are always changing, the IAM system must constantly adapt.

For that reason, the most successful IAM initiatives are run as ongoing programs, with permanently assigned staff and budgets, rather than one-off implementation projects. This enables organizations to keep up with change and also to drive user adoption—which is key to getting a return on investment.

2) Deliver New Functionality Frequently

Avoid the big bang approach: Don't take too long to stand up a system, because needs change constantly. If you take a year or more to implement IAM, you may find that the business processes and integrated systems have changed by the time you finish. A good rule of thumb is to deliver something meaningful every three to six months.

3) Measure Results

To justify an ongoing IAM program, it's important to measure user adoption and benefits. Identifying business drivers and the associated metrics can help calculate a return on investment. See sample metrics, Figure A.

4) Understand Your Users

Keep in mind that you have multiple user populations, each with distinct user lifecycles and business processes. For that reason, it makes sense to manage onboarding, deactivation, authentication, and access control for each population separately. As Figure B demonstrates, there are many possible deliverables for each segment of users.

5) Integrate, Integrate, Integrate

It's vital for an IAM system to integrate with a variety of systems campuswide. Possible integrations include: directories, e-mail systems (internal or hosted), student records systems, administration/finance systems, and research systems.

This year, consider adding new integrations to the mix:

- Automatic provisioning of user e-mail accounts on hosted e-mail systems from vendors such as Google or Microsoft.
- Enabling students, especially in computer science and related disciplines, to provision and de-provision virtual machines on cloud providers such as Amazon EC2.

6) Leverage Student Labor

Higher education organizations often have low budgets—particularly in today's economic climate. Fortunately, they also have a plentiful supply of inexpensive labor for implementing IT systems: students!

Utilize student labor for such tasks as business analysis, integration work, and implementation of business logic—not just initially, but on an ongoing basis. Students can help deploy a first-phase system, evolve the system's capabilities, and then transfer their knowledge to the next generation of student workers, supplying some of the work to make your IAM initiative a long-term success.

About the Author

Idan Shoham *is founder and CTO of Hitachi ID Systems.*

	USER POPULATION			
Process	Students	Faculty	Staff	Alumni
Automated onboarding	X	X	X	X
Automated deactivation	X	X	X	X
Request-driven workflow	?	X	X	?
Enrollment of contact info	X	X	X	X
Enrollment of security questions	X	X	X	X
Self-service password reset	X	X	X	X
Password synchronization	X	X	X	X
Privileged ID management	?	X	X	

FIGURE B

The Organization

Berry College
2277 Martha Berry Hwy NW
Mount Berry, GA 30149
www.berry.edu

The Challenge

Optimizing and managing use of existing bandwidth

The SonicWALL Solution

SonicWALL E-Class Network Security Appliance (NSA) E6500 Next-Generation Firewall

The Results

- Greater insight into application traffic
- Granular bandwidth control
- Savings through consolidation

Vendor-Sponsored White Paper

NETWORK SECURITY: Berry College Case Study

Founded in 1902 near Rome, Georgia, Berry College is an independent, coeducational college that provides approximately 1,850 students with undergraduate degree programs in the sciences, humanities, arts and social sciences, as well as undergraduate and master's level opportunities in business and teacher education. The college employs approximately 600 faculty and staff members.

The challenge: optimizing and managing use of existing bandwidth

Over the past three years, the college went from one ISP and 40 MB connectivity to two ISPs and 200 MB connectivity. Simultaneously, the college experienced an upsurge in streaming video, game consoles, DVD players, smartphones and tablets. The corresponding bandwidth consumption is especially problematic during classes and peak study hours.

Vendor-Sponsored White Paper

"SonicWALL lets me see all the way down to whether someone is watching a show on Hulu or a viral YouTube video, or transferring a lot of files over IM. That's a huge improvement over the visibility we used to have." – Dan Boyd, Senior Network Architect

As bandwidth and usage grew exponentially, the college began to consider a consolidated enterprise-class solution.

"There's a point at which simply adding more bandwidth isn't the answer. You need to implement smart tools to intelligently manage what you have," said Dan Boyd, senior network architect at Berry College.

Previously, the college had to check and maintain a separate IPS, traffic shaper and firewall, which increased administrative costs, and required additional monitoring. Berry College wanted to optimize existing bandwidth, simplify troubleshooting, boost performance, and gain the firewall capability to connect multiple ISPs to the WAN.

"We need to control applications, not just for legal reasons, but for prioritizing bandwidth," said Boyd. "Streaming content like Netflix and Hulu steals a lot of bandwidth from other applications, especially during class time when students are trying to get legitimate work done."

Boyd decided against selecting a WatchGuard® XTM 1050, noting, "WatchGuard had a hard time dealing with our mix of traffic."

Instead, Boyd selected a SonicWALL® E-Class Network Security Appliance (NSA) E6500 Next-Generation Firewall from reseller Carolina Advanced Digital, Inc.

In addition, the NSA E6500 offered multiple ports and High Availability (HA) configuration for greater connectivity and reliability. Boyd could also offload features onto the secondary device to keep CPU cycles down on the primary device. Boyd had experience deploying SonicWALL products for over 10 years.

"SonicWALL has consistently offered a better value for the money than similar solutions we've looked at," reported Boyd.

The solution: SonicWALL E-Class NSA E6500 Next-Generation Firewall

SonicWALL E-Class Network Security Appliance (NSA) E6500 Next-Generation Firewalls scale to the needs of expanding enterprises, featuring Application Intelligence and Control with real-time Visualization. Combining SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI) with a multi-core platform, it is configurable to analyze and control thousands of unique applications, whether unencrypted or encrypted with SSL.

The result: greater bandwidth control and application visualization

Migration to the new NSA E6500 appliances went smoothly, with only five minutes of downtime.

The consolidated SonicWALL solution has saved the college several thousand dollars a year in licensing by eliminating two additional IPS appliances, two additional traffic shapers, and four Cisco® routers. It has also considerably eased administration.

While Boyd uses SonicWALL ViewPoint reporting for historical trends, visualization enables him to identify and troubleshoot application issues in real time, even with full security measures in place.

"We have no direct control over student computers, but with SonicWALL's real-time visibility, we can see exactly what is going through port 80 regardless of whether it is web surfing, file transfers traffic or streaming video," said Boyd. "It spreads the troubleshooting load and lets everyone see what's going on from the central console and deal with it."

Boyd has prioritized bandwidth for core services including the college web site, student information system, student web interface, web-based student publications, and e-mail services. In addition, about 18 months ago, the college shifted from primarily being a consumer of inbound content to also being a provider of outbound media content (including web-based streaming video), which relies on prioritization.

"It's not a dramatic amount but we have to guarantee it goes out," said Boyd.

Boyd's team uses the SonicWALL Application Flow Monitor to visualize the network traffic on a daily basis to see not only who is using up bandwidth, but also how they are using it. If there is a network problem, Boyd can see precisely what is going on.

"SonicWALL lets me see all the way down to whether someone is watching a show on Hulu or a viral YouTube video, or transferring a lot of files over IM," said Boyd. "That's a huge improvement over the visibility we used to have."

SonicWALL Benefits

- Granular application intelligence, control, and visualization
- Gateway anti-virus, anti-spyware, intrusion prevention, anti-spam and content filtering
- Deep Packet Inspection of encrypted SSL traffic

The future: granular application control and high availability

Boyd plans to configure the two NSA E6500 devices in an HA pair to ensure ongoing reliability.

"Unless we triple our bandwidth in the next couple years, I don't see us growing out of them," reflected Boyd. "But the next time we evaluate new networking solutions, we'll look at SonicWALL first."

Boyd also sees great potential for policy-based and time-based control over social media traffic, not only in the classroom, but also for staff members who manage the college's Facebook and Twitter accounts. Going forward, Boyd will be incorporating Single Sign-On (SSO) functionality and establishing policy enforcement based on users and groups.

"We look forward to being able to identify and control policy based on detailed traffic information. This will let us determine, for example, whether a bandwidth spike is originating from a faculty member or a student working for a faculty member," concluded Boyd.

Vendor-Sponsored White Paper

THE COLLEGE AT OLD WESTBURY STATE UNIVERSITY OF NEW YORK

NEXT-GENERATION FIREWALL: SUNY College at Old Westbury Case Study

State University of New York (SUNY) College at Old Westbury is located on a 607-acre campus 20 miles from New York City. SUNY is comprised of 64 campuses statewide with an enrollment of 467,845 total students. The College employs over 250 faculty members and 300 non-faculty staff, and serves over 4,300 students, a quarter of whom reside on campus.

Typically, hackers do not target the College's network for proprietary information (as they would target research institutions or for-profit corporations). However, hackers constantly probe the network in attempts to steal identity and financial information, and leverage the network's high-bandwidth chain of thousands of devices as a hidden launching ground for outbound attacks.

The Organization

SUNY College at Old Westbury
223 Store Hill Road
Old Westbury, NY 11568
www.oldwestbury.edu

The Challenge

- Explosion in social media and increased demand for bandwidth

The SonicWALL Solution

- SonicWALL E-Class NSA E7500 Next-Generation Firewall

The Results

- Increased traffic transparency
- Optimized bandwidth management
- Higher service levels and user satisfaction
- Greater system reliability

"We look like a honey pot to the bad guys," said Marc Seybold, CIO at Old Westbury and current chair, SUNY Council of Chief Information Officers.

In addition, both students and staff own and operate a myriad of personal computing devices to connect to the College's local network and wireless services, and to the Internet via a third-party managed Internet service provider. Users expose their devices to threats off-campus and on the Internet, and then return to campus with the potential to compromise the College's network.

The challenge: explosion in social media usage and increased demand for bandwidth

SUNY College at Old Westbury experienced a profound increase in bandwidth, which stressed its existing legacy hardware beyond its technical capabilities and architecture. Seybold began evaluating alternative solutions that could provide firewalling, edge routing, and system redundancy in a cost-effective manner which would meet his budgetary requirements. In particular, he sought a solution that provided granular policy controls so that the College could better optimize its available bandwidth and tie traffic flows to particular users and groups.

"Faculty members often couldn't stream video properly in the classroom because we had hundreds of students consuming bandwidth on YouTube," said Seybold. "Since we couldn't tie users to traffic, we could only blanket-throttle all traffic, but as a result, the faculty still didn't get the performance they needed."

After extensive research and evaluation, the College selected the SonicWALL® E-Class

Vendor-Sponsored White Paper

"It made sense for us to be proactive and actually look at how the available bandwidth is being used over different time slices during the day, by user and then optimize it."

– Marc Seybold, CIO at Old Westbury and Chair SUNY Council of Chief Information Officers

Network Security Appliance (NSA) E7500 Next-Generation Firewall in paired High Availability (HA) mode.

"My memory of SonicWALL had been from back when it was just a SoHo vendor," said Seybold, "so I was very pleasantly surprised by the enterprise-level engineering and performance of the E7500."

The solution: SonicWALL E-Class NSA E7500

For organizations with large networks, such as the College, the SonicWALL E-Class NSA E7500 can provide Application Intelligence, Control and Visualization, gateway anti-virus, anti-spyware, intrusion prevention, anti-spam and content filtering. Combining SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI) technology with a high-performance multi-core platform, the NSA E7500 is configurable to analyze and control thousands of unique applications, whether unencrypted or encrypted with SSL, and without introducing latency. As an inline solution, the NSA E7500 leverages existing infrastructure while adding an extra layer of network security and visibility. As a security gateway, it adds secure remote access and high availability.

Unexpectedly, the previous firewall died minutes before SonicWALL technicians had arrived to begin setting up a parallel E7500 configuration. They managed to have the new E7500 solution operational—and the campus network back online—within a couple of hours.

"It was a pretty impressive response," said Seybold. "We have been very happy and satisfied with the service and support."

The result: greater transparency and control

The NSA E7500 helps Seybold shape and optimize bandwidth over his gateway firewall. With the E7500, Seybold is now able to view traffic flow and match it to specific users, adding a new level of transparency and control. This enables the College to protect network users and institutional assets, while enabling faculty and students to accomplish their work, unimpeded.

"When you consider how much student use of bandwidth-hogging social media applications, audio and video files has increased, it's clear that at some point any campus is going to reach its limits in terms of budget for additional bandwidth," said Seybold. "It made sense for us to be proactive and actually look at how the available bandwidth is being used over different time slices during the day, by user and then optimize it."

In addition, Seybold has found management to be easier than that of the previous solution.

"Our experience has been outstanding. Management of the firewall is much easier and technical support has been great," said Seybold.

The future: optimized bandwidth management

The College is looking forward to leveraging the NSA E7500 Next-Generation Firewall to provide even more granular bandwidth management and controls, based upon user, time-of-day, applications, and other behavioral factors.

"Our ultimate goal is to help our users optimize their network experience by shaping their own behaviors, rather than having to impose behavior on them," said Seybold.

SonicWALL Benefits

- Application intelligence, control and visualization
- Granular security policy enforcement
- Enterprise-grade performance and scalability
- Ease-of-deployment
- Ease-of-management
- Signature database of over 3,000 applications and millions of malware threats

About Us

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 Campus Technology

Campus Technology is a comprehensive resource that includes a monthly magazine, website, newsletters, webinars, online tools and in-person and virtual events—providing in-depth coverage on the technologies and implementations influencing colleges and universities across the nation. You'll discover valuable how-to content, best practices, industry trends, expert advice and insightful articles to help administrators, campus executives, technologists and educators plan, develop and successfully launch effective IT initiatives. Visit our booth to sign up/renew your FREE magazine or newsletter subscriptions and to set up your *CampusTechnology*.com online account to access the FREE resource tools exclusively found on our website.