IDC Government Insights

IDC VENDOR SPOTLIGHT

A Perfect Security Storm Challenges Higher Education

December 2011

Jan Duffy

Sponsored by SonicWALL

New technology has an amazing ability to educate and wired campuses contribute untold value to the learning process, providing the opportunity for everyone to voice opinions, share ideas, and connect with others. However, university and college administrators and technology managers know that this rich learning environment does not come without challenges and risks. It is not unusual for the typical higher education institution to have between 25,000 and 70,000 networked devices attached to very high speed, high capacity networks with fast connections to the Internet and to regional, national and international research networks. Many of the computing devices on the network are neither owned nor managed by the school and represent a wide range of configurations and applications. In some cases, the devices and applications are immature and untested, representing an unknown set of vulnerabilities. This situation is compounded by a user community — students, faculty, and administrators — with differing, sometimes conflicting, views on the level and type of security required. In this complex environment, maintaining a culture of open information exchange and optimized learning while protecting networks (and the devices attached to them) from abuse is not an easy task.

What Makes the Higher Education Computing Environment Different?

Colleges and universities exist in a highly competitive market; they actively vie for students, faculty, funding and research projects. Student enrolment is exploding, but the financial resources are eroding. Funding models are changing; in some instances students are now paying a much higher premium for higher education than in the past and this heightens the expectation for services.

It is not unusual for professors to post quizzes, homework assignments, tests, and lecture notes online, all of which must be protected from unauthorized access and distribution. In today's world, the learning and exploring that represent the primary activities of higher education institutions is best supported by networked computers, access to information, and real-time communication and collaboration.

Free access to information is vital, but there is a fine line between freedom of information and the risk of information abuse or loss. Universities and colleges have had difficulty enforcing IT policies and the result has been a number of serious data breaches. Hackers probe university networks in attempts to steal identity and financial information and leverage the network's high bandwidth and the many attached devices as a hidden launching ground for outbound attacks.

Proprietary information is crucial to any research institution, it leads to recognition, rewards, prestige and funding and its theft or misuse could deal a devastating blow to the long-term viability of the institution. This highly prized content must be accessible to professors, researchers and students without the risk of a security breach.

Diversity, change and the need for compliance — a perfect security storm

Often on the cutting edge of innovation, higher education institutions face three unrelenting challenges that represent a perfect security storm — a diverse group of users, constantly changing technologies and threats, and increased compliance and data protection pressures — a storm that can result in dire consequences. The situation is compounded by network complexity, a constantly changing threat landscape, remote access from non-managed devices, aging security systems, a culture of open information exchange, a large portion of the user population that is technology savvy, and budgets that continue to be cut. The result is a high incidence of

information security incidents ranging from laptop theft, copyright infringement, denial of service attacks, bot infections, and unauthorized access to data, systems and networks.

The solution is a system that protects the network from viruses and other malware as well as from unauthorized access, provides secure remote access from all types of devices using any type of Internet access, secures wired and wireless networks equally well, prevents data leaks and ensures regulatory compliance, and last but not least a security system that is easy to manage and is affordable for today's cash-strapped higher education institutions. But before we talk any further about the solution, let's talk about the challenges a little more.

Different Users, Different Characteristics, Different Needs

Every computer security professional is concerned about internal and external attacks, but this concern is greatly amplified in a campus environment, where many different users with different characteristics and different needs have physical access to the computers and networks. Regardless of the type of higher educational institution, the technology user groups are diverse, with different characteristics and varying needs. The user population is often categorized in the following way:

- **Management, administrative and technical staff.** Generally speaking, this group of users remains relatively stable and is likely to share geographic proximity. Although there may be some use of personal devices, much of the technology used by this group will be provisioned by the institution and is therefore easier to secure. Adding SSL VPN access to the devices and network used by this group is a conventional approach to enabling remote access to network resources. However, this group is likely to access the most valuable and proprietary assets of the institution which increases the level of priority and affects the type of security required.
- **Academic faculty, including visiting professors and researchers.** A mix of permanent and transient individuals, faculty and researchers are accustomed to sharing information in a quick and easy way without the need to deal with restrictive computer policies and tools. Although institutions are now inclined to take a more restrictive approach to information access, the culture in most higher education institutions remains one of open networks and freedom of information exchange.

  In addition to this "open information sharing" environment, faculty use networked electronic educational applications such as anti-plagiarism tools, social bookmarking applications, assessment tools, online exam applications, content creation tools, and student information and notification systems to enhance the learning experience. These are commonly used in conjunction with a variety of technologies, such as podcasts, online social networks and other Web 2.0 applications, smart boards, wireless projects and PCS that are fully functional endpoints or primary purpose terminals, all integrated with enterprise level learning management systems (LMS) to provide seamless access to online learning. This introduces an additional level of complexity to information security.

- **Full and part-time student body, including exchange students, and off-campus students.** The student body may turn over several times each year. Students are technology savvy and are accustomed to having access to information sources on an unrestricted basis whenever and wherever they are. Students arrive on campus expecting to use mobile apps on their smart-phones and tablets to navigate campus resources and use campus services. This trend is likely to continue as mobile options and related costs continue to decline.

  Today's students have been using personal computing devices as the basis for much of their communication for a number of years and network usage habits, including the use of applications considered to be high risk from a security perspective (e.g., P2P, instant messaging) have been acquired and become engrained in this time. It is unlikely that these habits support the institution's recommended practices, experience has shown that automatic enforcement of computing and information security is the preferred approach when dealing with the student body.

- **Conference attendees and other guests.** Guest lecturers, alumni, students' parents and conference attendees are a transient group that may request temporary email accounts, access to computer labs and network printers, Internet access, or access to information housed in the institution's computers for official and personal use.

Constantly Changing Technology Landscape

The technology landscape continues to change, and the use of new technologies, even untested and unproven models and applications, is not uncommon in the higher education environment. With the unprecedented success and continued growth in the use of personal computing devices, including laptops, smartphones, WiFi only devices such as the Apple iPod touch, wireless game controllers, tablets, and so on, universities have to manage a very complex environment. Whereas four or five years ago, most students arrived on campus with just one personal device, it is not unusual today for a student or faculty member to own two, three or four wireless-enabled mobile devices based on one or more operating systems. In some cases, devices emerge and are in use before universities have the opportunity to consider how to secure them. It is rare for universities to ban the use of a device, but regulation of new devices could become more commonplace as they trade flexibility for security.

The number of Web-based applications that higher education users rely on and access from the school network continues to increase at a dramatic rate. This is due in part to the emergence of Web 2.0 technologies in conjunction with individual-liable devices, such as smartphones that are purchased outright by the individual user and that do not form part of the official technology set endorsed by the school. This has driven an increasing number of threats and vulnerabilities. One of the most difficult challenges is to balance the use of productive applications versus non-productive and potentially damaging applications.

It is no longer enough to blacklist or white list applications. Parts of a Web application may open the network to vulnerabilities, but other features offer value. A new approach to network security is needed to reflect threats posed by Web 2.0 applications. For example, there is a need for granular application control that supports policies that allow Facebook access for certain groups or individuals while disabling features that have no value or that present opportunities for data leakage. At the Old Westbury Campus of SUNY College, faculty members often had difficulty streaming video properly in the classroom because students' use of YouTube consumed bandwidth, but were unable to tie users to traffic so were required to disable access on a blanket basis. The result was unhappy students and unhappy faculty until the college implemented a new security system that provided granular bandwidth management and controls, based upon user, time-of-day, applications, and other behavioral factors.

From an infrastructure perspective, cloud-based services offer significant operational and financial benefits to higher education institutions — as well as benefits for research and high performance computing — and there is increasing interest in using cloud, particularly for non-critical applications such as email and calendar as well as LMS and CRM services. Extending infrastructure beyond the institution's perimeter increases the criticality of traffic. The use of bandwidth-hungry applications can hinder network performance and ultimately reduce access to mission-critical applications. Securing this environment requires a high speed system that can perform inspections in real time.

When Berry College in Rome, Georgia, went from one ISP and 40MB connectivity to two ISPs and 200 MB connectivity there was a surge in streaming video, game consoles, DVD players, smartphones, and tablets. The corresponding bandwidth consumption became problematic during classes and peak study hours and required a consolidated enterprise solution to help them manage this situation intelligently. A consolidated solution saved the college several thousand dollars a year in licensing, but most importantly, with real time visibility it allowed the network administrator to visualize the network traffic to see who was using the bandwidth and how it was being used.

Regulation and Compliance

Compliance relates to the legal obligations that a university or college has to secure information. Private and public information security regulations are often the starting point for an information security strategy. The wide variety of sensitive data held in higher education databases subjects them to a very broad range of compliance regulations. The university processes information about staff and students for various teaching, research, and administrative purposes. Personal data are processed according to the regulations of a specific jurisdiction. It is important for higher education institutions to be familiar with current compliance regulations and to ensure that computer security policies and systems are updated to maintain the institution's integrity in this regard. Unfortunately, there continue to be student data breaches that could have been avoided, had the security of the IT system been more suited to purpose.

Certain data warrant particular attention; for example financial data, including information about financial aid, medical records, and other proprietary data sets such as student records. These data are highly sensitive, and

governed by specific private and public information security regulations. Following is some of the U.S. legislation that needs to be carefully considered along with any other pertinent state laws in a higher education institution's security infrastructure:

- The Family Educational Rights and Privacy Act (FERPA) is a U.S. federal law that protects the privacy of and right of access to student education records.
- PCI Security Standards (including PCI-DSS and PCI-DA) govern the payment card data security process.
- The Children's Internet Protection Act (CIPA) is a U.S. federal law that requires schools and libraries that receive federal funds to adopt and implement filtering systems to block specified sites.
- The Health Insurance Portability and Accountability Act (HIPAA) governs security regarding personally identifiable medical information
- FIPS, FISMA, Common Criteria and other relevant regulations related to services provided to the Federal Government or under Contract
- The Gramm-Leach-Bliley Act (GLBA) governs the security of any record containing nonpublic financial information about a student or other third party who has a relationship with the higher education institution.

Mitigating the Risks, Regaining Control

Major virus and worm outbreaks can be extremely disruptive and can bring a university network to its knees, crippling day to day operations and requiring enormous cleanup efforts. Realistically, it is impossible for higher education institutions to avoid devices arriving on campus with worms and viruses, but it is possible to prevent these security risks from spreading and affecting the entire network.

To protect against threats, it is important for higher education institutions to stop breaches before they happen through a well designed system of network access control and identity management. It is unlikely that everyone who works on or visits the campus can be persuaded to install appropriate up to date antivirus software, so it is important for every device attempting to log on to the network to be examined to verify that it complies with campus security policies; for example, that it has an up to date operating system and antivirus software installed regardless of whether the student is using university approved software. If a student device requires a patch or an update, this needs to be remedied before it can affect the rest of the network.

Next-Generation Firewalls and Content Filtering

Given all the constituencies and different levels of security required, higher education demands an intelligent, flexible security system that can be managed centrally. The old notion of a perimeter must be replaced with the inverted network approach, secured by gateways. This includes IP, WAN and LAN ports, plus secure wireless access. SSL VPN technology must be implemented to ensure staff productivity when offsite and IPSec solutions used for site to site networking. If the network includes remote users, SSL VPN is a must. Security can be pushed even further, out to the endpoints of systems that are managed by the institution and systems that are not managed by the institution. This requires intelligent gateways that can recognize the secured devices, perform automated maintenance and, again, be centrally managed.

IDC classifies the firewall as a security product with the primary function of general purpose filtering of networking traffic, using one or more of the following: packet filtering, stateful inspection or proxy. Virtual private networking capabilities are featured in some products, and firewall/VPN security appliances may also host other security features. Appliances that layer additional security mechanisms and features onto a single device are becoming mainstream. They are based on the traditional firewall or UTM appliance but have additional features such as content inspection, application intelligence and control, and even networking functionality.

Enter the next-generation firewall (NGFW). The NGFW market is comprised of security products that include multiple security features integrated into one device; the appliance must have the ability to perform network and application firewalling, network intrusion detection and prevention, and gateway antivirus (AV).

Visibility and End-to-End Control of the Network — Implementing the Right Processes and Controls

Since Web 2.0 applications including collaboration and social networking are creating more network dangers, security architecture needs to encompass more than the network perimeter. Higher education institutions need security that focuses on specific applications, user authentication and quality of services. IT must monitor and control data, applications, devices, networks, and user access. Mobility, virtualization, social networking, VoIP

and unified communications are all impacting the network and creating a need for a more holistic security approach. The sophistication of attacks, complexity of security solutions volume and complexity of network traffic are all increasing. The traditional patchwork nature of network security is often inadequate. The NGFW provides multiple protection mechanisms and features designed to prevent threats/attacks from network to application layers.

Deeper and Tighter Inspection of all Content

The reality of security today is that deeper inspection of all content is essential versus just the application allow/deny approach offered by some network gateway and firewall products. Application intelligence and control provides protection, management, and control over application-layer traffic allowing IT administrators to maintain granular control of applications and users. Administrators can easily create bandwidth management policies based on logical pre-defined categories (such as social media or gaming), individual applications, or even users and groups. As new applications are created, new signatures are pushed to the firewalls and the appropriate policies are automatically updated without IT spending costly time and effort to update rules and application objects. In addition, administrators can use granular application-based policy to restrict or block the transfer of specific files and documents, prioritize or throttle bandwidth and deny access to internal or external Web sites.

The focus is on scrutinizing the content of legitimate applications and on blocking unwanted applications to ensure threats are not passed via application communications; even trusted applications are continuously monitored to ensure the application's behavior or content is not malicious. Integrated application intelligence and control ensures granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity. The NGFW with these features tightly integrated offers an economical, secure, and easily managed option for the higher education institution, allowing inspection of traffic in real time regardless of port or protocol and regardless of file size.

What Makes the NGFW Solution a Viable Alternative

The complexity of the higher education institution demands an integrated, cost effective network security solution that has the flexibility and scalability to manage the complete security solution from one location. The conditions making enterprise NGFW an appealing network security solution include the following:

- Attackers/defenders arms race requires advancing technology with consolidated management, content inspection, routing, application awareness, and granular security policy enforcement.
- Reducing network complexity and risk
- Common command structure to reduce the risk of poor configuration
- Consolidate knowledge of security status within network
- Aggregated reporting for policy compliance
- Appliance-based approach means one box can handle blended threats, or multiple boxes can be centrally managed

Securing the Data, the Network and the Users with SonicWALL Solutions for higher Education

The explosive adoption of technology in higher education has changed the network as we know it. The perimeter has disappeared along with traditional ways of interacting with applications. This is the result of many trends and technologies including:

- Universal use of mobile computers, plus other network attached devices like handhelds, tablets, and mobile phones
- Remote user access to information resources
- Centralization of datacenters to support more diverse access
- The deliberate move to cloud computing and cloud storage
- Virtualization or the use of Web 2.0 functionality that both accesses and generates stored data

All of this has led to a dramatic increase of security challenges. However, the strategies and tactics to address them are less apparent. This is especially the case when an institution's IT budget is allocated between different schools, campuses, and even departments. While this budget distribution provides resources to tailor security

solutions on the "front lines", it can adversely impact IT's ability to address the increasing number of vulnerabilities.

Aligned with higher education security and user experience requirements, SonicWALL solution capabilities include the following:

- **Intelligent, Highly Adaptive Security.** SonicWALL next-generation firewalls scan every byte of every packet for the deepest level of protection and scale to extend security to growing and distributed enterprise networks. SonicWALL's NGFW offers security combining gateway content filtering, antispam, antivirus, antispyware, intrusion prevention, and application intelligence and control. This supports the higher education institution's need for intelligent, highly adaptive security.
- **Massively Scalable Multicore Architecture.** The SonicWALL SuperMassive E10000 Series is SonicWALL's next-generation firewall designed for large networks to deliver scalability, reliability and deep security at multigigabit speeds. Application traffic analytics allow for the identification of productive and unproductive application traffic in real time, which can then be controlled through powerful application-level policies. The solutions can secure enterprise networks, datacenters, and server farms, and meet the needs of higher education for threat protection including intrusion prevention and low latency malware protection.
- **Secure Network Traffic Controls.** SonicWALL's unified threat management firewall gateway appliances provide institutions with a secure network free from viruses and other malware. Unauthorized access to a university network could jeopardize day to day operations. The firewall provides the first line of defense against Internet security attacks. The SonicWALL E-Class Network Security Appliance (NSA) Series is engineered to drive down administrative complexity, while defending against network attacks, both externally and internally, at high speed. NSAs offer centralized management, network segmentation, multiple deployment options and advanced networking features for control and flexibility. Combining multicore technology with unrestricted deep packet inspection, NSAs are the most scalable, reliable and highest performing multifunction unified threat management appliances in their class.
- **Secure Remote Access.** With the profusion of Internet accesses (xDSL, WiMAX, cable, satellite, new 4G, etc.) and the consumerization of IT devices (laptops, netbooks, smartphones, etc.) combined with heightened focus on remote access for disaster preparedness and business continuity, secure remote access is imperative to today's learning environment. But in order to increase productivity and reduce IT overheads, the successful solution must also be easy for both users and administrators. SonicWALL E-Class Aventail SSL VPN appliances provide ease of deployment and usage plus granular control and connection to a wide range of leading end-point devices.
- **Secure Wireless.** SonicWALL's aim is to make wireless networking secure, simple and affordable with the SonicWALL Clean Wireless Solution — which integrates 802.11n and 802.11a/b/g wireless management with unified threat management (UTM) security and application firewall to provide application-based policy control. The SonicWALL Clean Wireless solution designed to give organizations the confidence that their wireless network is as secure and well managed as their wired network.
- **Email Filtering and Anti-spam.** With increased sophistication and complexity of inbound email threats, organizations need a powerful, integrated, yet easy to use email security solution that can effectively prevent inbound and outbound email threats. SonicWALL E-Class Security solutions provide protection against spam, virus and phishing attacks, information leaks and violations of regulatory compliance laws.
- **Identifying and Addressing Network Vulnerabilities.** Geographically-distributed sites exacerbate the costs and challenges of enabling distributed learning with a minimal administrative learning curve. A global management system facilitates the management of SonicWALL firewalls, backup and recovery, secure remote access, and email security appliances from a single location. GMS also allows the IT administrator to monitor their SonicWALL infrastructure and create reports necessary to comply with information security regulations. The SonicWALL Global Management System (GMS) provides centralized policy-based network security management, active monitoring and reporting, that can scale up to thousands of locations. SonicWALL's Management and Reporting Solutions provide architecture for centrally creating and managing security policies, providing real-time network monitoring and event logging, and delivering intuitive compliance and usage reports from a single management interface. Customers can use GMS either on a third-party Windows-based server or on the SonicWALL Universal Management Appliance.

Conclusions

The network security needs of higher education institutions are ever-changing and vendors that want to remain successful must adapt. Organizations are demanding great flexibility in the solutions they purchase. Acquiring an additional box for every new threat that is identified is no longer an option. Companies want to know that their investment will be protected and will scale as they grow. Increasingly integrated solutions and virtual security appliances are being considered to address these needs.

Organizations are also demanding more granularity in setting policy. It is not enough to limit access to a particular resource based on department. Companies want to zero in on not only the individual but even the device that person is using to access the network. To this point, centralized management platforms are necessary to keep policy and security product control efficient and streamlined, and serve as a differentiator between vendors.

The external threat landscape is changing. Attacks are becoming more targeted and malware more varied. Signature-based solutions lose effectiveness in this environment. Rather, products that look at reputation and use heuristics and behavioral pattern recognition are better positioned to weed out unwanted traffic on the network or prevent it from gaining entrance in the first place.

As Web-based applications continue to proliferate, networks will face an increasing number of threats. Since many employees rely on Web-based applications, organizations in many cases cannot blacklist applications outright. Instead, organizations have to take a more granular approach to network security by implementing application control along with the more traditional filtering functions associated with firewalls.

A new generation of security solutions is emerging that builds on the traditional functionality and is targeted specifically at the enterprise. These new devices enable organizations to deploy a single box for their network security need, or deploy multiple boxes with centralized management.

To the extent that it addresses the challenges mentioned in this paper, IDC Government Insights believes that SonicWALL can succeed in this important and growing network security market, competing successfully against large, well established incumbents that have been working with higher education institutions for some time.

About SonicWALL

SonicWALL Inc. is a San Jose, California-based provider of network security and data protection products. SonicWALL solutions are designed to protect networks from intrusions and malware attacks through hardware, software and virtual appliance-based solutions.