A CAMPUS TECHNOLOGY
CUSTOM WHITE PAPER

www.campustechnology.com

BUILDING OPEN AND SECURE WIRELESS NETWORKS ON CAMPUS

4 Best Practices for Wireless LANs

Table of Contents

Introduction: Wireless Is Integral to Education Today

With academic institutions in the U.S. spending more than $5 billion annually on the hardware, software, and services that make up wireless networks—and with that figure expected to climb—interest in wireless access on campus is at an all-time high[1]. The accelerated adoption of wireless technologies and devices on campus is a clear trend in higher education, and can help both save on the cost of extending the network and competitively differentiate an institution.

Today, providing fast, ubiquitous Internet access for the multitude of devices used in higher education has become a necessity on university and college campuses. In fact, mobile devices continue to proliferate—including netbooks, smart phones, laptop computers, e-book readers, and more—with many students carrying multiple devices, some issued by the institutions themselves. With universal connectivity imperative, the cost-effective way to provide Internet access virtually anytime, anywhere it is needed is through wireless. For example, it is far less expensive to outfit a 300-seat lecture hall with wireless than to install a wired connection for every single seat. The same applies to older buildings found on campus, where fixed network connectivity can be challenging and prohibitively expensive.

In a world where providing fast, ubiquitous wireless access is a given, securing those wireless networks properly is equally important. Because widespread wireless access has become integral to campus life, it is no longer possible to constrain the wireless network's range or capacity in order to limit exposure, retain control, and ensure security. Rather, wireless networks must extend everywhere and welcome guest access, while simultaneously ensuring that the overall network remains secure.

Fortunately, wireless security has matured and products and techniques are available to secure the network. Wireless networks remain vulnerable today not because the technology is not available, but because they are not securely deployed and maintained, making them ripe for an attack. Many administrators simply have not been properly trained to correctly deploy

[1] According to an 2010 report from Compass Intelligence, an IT consultancy and market research firm, education institutions—both K-12 and higher education—will spend $5.7 billion in 2010 on wireless services and equipment, growing at a compound annual rate of 5.2 percent through 2014. "Education Investments in Wireless Continue to Grow," David Nagel, Campus Technology magazine, Oct. 7, 2010, www.campustechnology.com.

Sponsored by:

BROCADE

January 2011

CAMPUS TECHNOLOGY

such networks–or have not been given the resources to purchase the right wireless network products and security tools.

However, campus network administrators can build and maintain secure wireless networks—and do so while maintaining the open networks that today's higher education institutions demand. This paper outlines four best practices for structuring open yet secure high-speed wireless LANs.

Best Practice No. 1: Prevent Peer-to-Peer File Sharing

A huge challenge on college campuses today is controlling peer-to-peer (P2P) file sharing, through which students use Internet connections, both wired and wireless, to illegally share large music and video files.

Institutions need ways to curtail illicit file sharing, which can bring the network to a standstill and make the institution liable for legal costs if it is not proactively addressed. The wireless network—due to its popularity with students—is often used for P2P activities, so it makes sense to integrate P2P security policies into the wireless firewall.

The simplest method is to block well-known network ports that are used for P2P activities. Wireless products that prepare reports on network security can then be used as proof that the institution has taken reasonable measures to block P2P access. So-called "rate limit" capabilities can also be used to control the exchange and downloading of large files through the firewall, but the most basic security method—for both wired and wireless networks—is to block those ports commonly used for P2P.

HOW A UNIVERSITY IS BLOCKING P2P FILE SHARING

One university customer has integrated Brocade® network security solutions into its wireless firewall, allowing the institution to both block illegal use by outsiders and enforce network usage policies by preventing illicit peer-to-peer (P2P) file sharing among users.

The campus, located in a highly populated metropolitan area, was exposed to many users carrying a wide variety and number of wireless devices. Network administrators needed a scalable way to do two things: block illegitimate users (including hackers), *and* stop legitimate users from using the network for P2P file sharing—an enforcement solution that would protect not only their data center and servers, but also their users.

Using the Brocade integrated wireless firewall, the university is now better managing its networks by blocking outsiders from illicit access, while also ensuring that permitted users—students—are not using the network for illegal file-sharing activities.

Best Practice No. 2: Shut Down Rogue APs

Rogue Access Points (APs) pose a serious threat to wireless networks. No matter how secure the wireless network, if someone with access—staff, faculty, or a student—deploys an unauthorized device, it can create a large security gap. Another challenge is so-called “soft APs,” which are becoming more prevalent. Soft APs can be run on laptops or smart phones, and are used to allow nearby wireless devices to share a wired Internet connection. Soft APs are considered rogue APs because they permit unauthorized devices or users on a secure network.

Controlling rogue APs can be a real challenge for wireless network administrators. Fortunately, a monitoring device is available that looks for specific security threats, helping to tightly monitor and control APs. Without such a dedicated monitoring device in place, it is impossible to tell if and when someone has breached the network with a rogue AP.

For higher education institutions, another challenge is distinguishing between true rogue APs and simple intrusions from homes or businesses on the outskirts of campus. In one real-world example, a university adjacent to a residential neighborhood needed to secure its wireless LAN in order to comply with data privacy laws. Specifically, the university needed to secure its wireless network to safeguard personal information on students and staff as well as financial operations information.

Preventing rogue APs from accessing the wireless network was a huge concern. Furthermore, because the university was using the 802.11n wireless standard, any rogue AP would be able to breach the network at even higher speeds and greater distances than was previously available with older wireless standards.

Mitigating the rogue AP threat was especially challenging in this case because the university needed to be careful to distinguish real threats posed by rogue APs versus a campus neighbor running a home wireless network.

The university turned to a rogue AP security solution specifically designed as part of its wireless intrusion prevention system. With that in place, network administrators not only were able to monitor and detect rogue APs, but also distinguish a true rogue AP from a friendly campus neighbor. Any mitigation steps taken against a rogue AP are not accidentally applied to a neighbor's home AP—even though the network detects many of these “friendly” APs on the perimeter of the network.

The wireless intrusion prevention system also works by applying rogue AP suppression from the wired side of the network. This blocks rogue APs from accessing the wireless network from the wired side, adding an extra layer of security in areas where wireless rogue AP suppression is not enough.

Finally, the university has the option of dedicating specific APs to monitor the wireless network—or dedicating one of the radios on a dual-radio or tri-radio AP. That means that rather than using time slicing, which checks only intermittently for rogue access, network administrators can assign a specific radio on an AP for constant around-the-clock network monitoring.

Rogue access detection systems also should provide reporting and auditing tools, thus helping institutions to complete required compliance paperwork confirming the security of the campus wireless network. In the event of a security breach, compliance regulations may require that a college or university produce proof that its network is securely designed—including that it monitors continually for rogue APs.

For example, the Gramm Leach-Bliley Act (GLBA) requires that colleges and universities be in compliance with Federal Trade Commission (FTC) rules regarding the safeguarding of financial information collected from students, such as financial aid information. GLBA requires institutions to take steps to ensure the security and confidentiality of records, including credit card and Social Security numbers. Similarly, student, faculty, and staff health information must be secured according to the Health Insurance Portability and Accountability Act (HIPAA). In the event of a network breach, higher education institutions may be called upon to prove that the networks—both wired and wireless—are secured appropriately. Providing reports that the network is routinely monitored for rogue APs can be part of that proof.

UNDERSTANDING WPA2

Although acronyms such as WEP (Wireless Equivalent Privacy) and WPA (Wi-Fi Protected Access) are popular in security discussions, many security standards that are commonly mentioned are not truly secure. Readily available tools on the Internet can enable an outsider to break into a WEP-secured network very quickly—and that includes networks using protocols such as Cisco’s LEAP and standard WPA, which are also insecure.

Instead, institutions should elect to use WPA2 with AES encryption as the primary method of deploying wireless security on their networks. WPA2 with AES standard is built into all 802.11n systems, but must be properly deployed when the network is set up in order to be operational.

Because it has authentication and encryption built in, network administrators will want to be sure to use the wireless security standard known as WPA2 CCMP. WPA stands for Wi-Fi Protected Access, a certification program developed by the Wi-Fi Alliance, a trade association. WPA2 is a more advanced and complete protocol introduced after the original WPA standard.

WPA2 is available in two versions. Be sure to choose the version of WPA2 that uses the encryption protocol known as CCMP—it is a mandatory part of the WPA2 standard and uses the stronger AES (Advanced Encryption Standard) encryption. The alternate version of WPA2, known as the TKIP version, uses WEP encryption, which is not as strong.

In summary, while wireless and security protocols are loaded with acronyms, the base rule to follow is simple enough: Use WPA2 with CCMP and AES

Best Practice No. 3: Lock Down Guest Access

Almost by definition, campus networks must be open not only to students, faculty, and staff, but to student families, visiting researchers, and others who need one-time or short-term access to the network from anywhere on campus. One of the most popular and necessary uses for wireless networks in higher education—and yet one of the most challenging—is enabling safe and secure Internet access for guests and visitors.

A good way to provide open but secure access is to deploy a separate guest portal into the wireless network. Higher education institutions could build a guest portal right into the wireless controllers, but they may also need to deploy a standalone guest portal. In either case, they will have a guest entryway that provides a browser-based way to control access into the network.

The guest portal is configured so that when a visitor opens a browser on campus and requests wireless access, the browser is redirected to a specific portal created for guests. That gateway to the network requires a user name and password, which is issued when the guest signs in on campus. Once the guest clicks to accept the terms and conditions shown on the portal, they are admitted as a secured user. This ability to easily build and control guest portal access should be included in the software offered by the college or university's wireless vendor.

With the right wireless product, institutions of higher education can also fortify security by creating different portals for different levels of guests. Certain vendors, for example, may need access to some financial data stored on the network, while typical guests do not.

Even with guest portals in place, network administrators should never assume that a secure tunnel into the wireless network means that anyone who is granted access to the network is harmless. Even with the right credentials, a guest "insider" can still be dangerous.

In anticipation of such an intruder, network administrators will want to inspect all user-generated packets. This requires placing an intrusion detection system that is part of the wired network *behind* the wireless aggregation point—usually the firewall between the wired and wireless networks. In this way, colleges and universities can still monitor the behavior of connected, authorized, and authenticated guest users on the wireless network to ensure their behavior is not malicious.

Best Practice No. 4: Continually Monitor Your Network

Once these wireless security steps are in place, higher education institutions will want to continue to monitor the network for illicit activity. The best way to conduct this continual risk assessment is through network scanning, using a network sniffing device. Look for rogue APs that may crop up, along with unauthorized users or misconfigured APs—in short, anything unusual that may indicate a problem and compromise network security.

Dedicated sensors offer an effective and reliable way to continually monitor the network. Rather than using time slicing, a technique in which a radio or an AP spends certain "slices" of its time scanning the network for problems, and the rest of the time connecting users, dedicated sensors can be set up to monitor the network continually.

Multi-radio APs provide a cost-effective way to integrate dedicated sensors into the wireless network. One radio out of two or three on an AP can be used for wireless sensing, while the other two radios act as conventional wireless transmitters.

Summary: Secure Your Wireless Network Now

In addition to the four best practices outlined in this paper, higher education institutions should consider acting on this final "short list" of items in order to jump-start their campus wireless security initiative.

Perform a wireless risk assessment and develop a policy in writing

Colleges and universities cannot know how secure their networks are unless they conduct a wireless vulnerability assessment. But they need to do more than just conduct the assessment—they need to document the findings and deploy a policy explaining how encryption, authentication, and auditing will be conducted on the wireless network. Then they need to synchronize this information with all of their risk management and compliance initiatives.

Continue to audit the wireless network regularly

Depending on the institution's compliance initiatives, the college or university may need to prepare a formal audit report on its network every quarter or every six months. In the meantime, their network administrators should use tools that will help continually audit the wireless network to ensure that it is securely deployed and performing well, and to check that no unexpected configuration changes have occurred.

Synchronize security with compliance

Higher education institutions will want to synchronize strong security policies with whatever other compliance policies they have in place—for financial privacy, handling of student health data, and much more—since there will probably be overlap. For example, a university's policy for handling credit card data collected by the bookstore should synchronize with its wireless policies for the university credit union. Or, wired and wireless policies for protecting student health records from the health center must mesh with campus health privacy regulations. In short, whatever organizational compliance objectives are already in place must tie into the institution's wireless security initiative.

Today's students expect robust, secure, and ubiquitous wireless networks that consistently perform well anywhere on campus. Providing reliable wireless access is essential to being a competitive higher education institution. Wireless networks provide a highly cost-effective option to wired networks for tasks as diverse as course delivery or smart phone access, voice over Wi-Fi, guest network access, netbooks, notebooks, e-readers, and more.

From dorm rooms to cafeterias to common areas to classrooms, with the right planning and tools, colleges and universities can make their campus wireless networks safe, efficient, and secure.

WALL OFF THE WIRELESS NETWORK

In the early days of wireless networks, APs were often connected directly to the main data center network. Within today's campus network, that type of open connectivity is a liability.

That is because once intruders breach an institution's wired network, they may have access to all sorts of internal information, including Social Security numbers, student health and financial information, and credit card numbers. For that reason, it makes sense to segregate the wireless network—where guests are allowed under certain controlled circumstances—from the more tightly controlled wired network. Therefore, along with the four best practices listed here, building a firewall between the wireless and wired networks is critical to constructing a secure wireless network.. Aggregate all wireless devices into a single point of access outside the firewall—a control point—and limit user access at that point to a few specific resources on the wired side.

Essentially, because there is a greater chance of unauthorized use of the wireless network, network administrators will want to wall it off from the rest of the network, setting up a clear demarcation between the two.

About Us

About Campus Technology

The only monthly publication focusing exclusively on the use of technology across all areas of higher education, Campus Technology provides in-depth coverage of specific technologies and their implementations, including wireless networks and mobile devices; enterprise resource planning; eLearning and course management systems; 'smart classroom' technologies; telecom, Web, and security solutions—all the important issues and trends for campus IT decision makers.

Targeting administrators, IT professionals and tech-savvy faculty, Campus Technology provides direction, analysis and detailed coverage of emerging technologies to assist technology leaders in their specific roles on campus. To learn more, visit www.campustechnology.com.

About Brocade

Brocade provides comprehensive network solutions that help the world's leading organizations transition smoothly to a virtualized world where applications and information reside anywhere.

As a result, Brocade facilitates strategic business objectives such as consolidation, network convergence, virtualization, and cloud computing. Today, Brocade solutions are used in over 90 percent of Global 1000 data centers as well as in enterprise LANs and the largest service provider networks. For more information, please visit www.brocade.com.