Next-Generation Network Security

Universities battle security threats with a layered approach

In the Middle Ages, city planners and feudal land owners relied on a multilayered approach to keep marauders at bay: Those laying siege to a castle, for instance, first had to cross a moat, then get past an outer wall, or curtain wall. If they succeeded in breaching this outer wall, invaders faced a series of daunting obstacles in a structure called a barbican, a narrow exterior passage that led to the main castle entrance. Invaders who were lucky enough to reach this barbican were subject to attacks with heavy stones, molten lead, or boiling water dropped through "murder holes" in the ceiling of the passage.

Their methods might not be as barbaric, but information technology officials at many colleges and universities have adopted a similar strategy in securing their computer systems from attacks. The routers, firewalls, and virtual private networks (VPNs) in their arsenal are analogous to the moats, curtain walls, and barbicans of old.

"A layered approach to security is desirable, because you are protecting yourself against a failure by any layer," says Julian Y. Koh, manager of network transport, telecommunications, and network services for Northwestern University.

Network Security, page 14

Network Security...

continued from page 13

"Let's say someone was able to get through the protective measures at our border router; they would still be blocked at the firewall level," Koh explained. "Or, if someone bypassed our border router and tried to come in through the VPN, the security measures at the VPN would stop them."

He added: "The layered approach is a way of protecting yourself against failure by any of the components in your security model."

Network security a growing challenge

College and university officials must deal with a host of potential threats to their network environments, with new online interactivity such as peer-to-peer communication, text messaging, and social networking contributing to the problem as information is shared across devices and networks.

A campus network can have thousands of devices logging in at any given moment, and security threats abound. College students, young and—by nature—typically curious, often test the security system just to see if they can crack it. More malicious attacks also can take place as hackers attempt actions such as stealing Social Security and credit card numbers, illegally accessing the student information system to change grades or destroy proprietary school information, or hacking into the financial system to make it look like tuition has been paid when it hasn't. Then, there are attacks launched unknowingly by users logging on to the network with their own machines that already might have been compromised by viruses and worms.

In short, every single device connected to the network—whether in a classroom, dorm room, administrative office, or off campus, as well as the smart phones and other web-enabled mobile devices that students carry around with them—is a potential entry point for a security attack.

With these developments, the chief information officers of higher-education institutions face a challenge that is perhaps greater than at any time in the past. Yet, at the same time, college and university CIOs also need to pave the way for users to access information from any location. Students and faculty want to be able to log onto the network using a variety of devices, from Macs and PCs to laptops, iPads, and smart phones. They need to be able to access the network from a variety of locations, both on and off campus. Distance learning, in particular, has made it more important than ever that students be granted access to resources from remote locations.

"Security is a wide-ranging topic," says Troy Herrera, senior marketing manager for Juniper Networks, a company that provides network security solutions for colleges and universities. "You want to make things accessible and encourage the sharing of information, but you must protect proprietary information and research and infrastructure."

Campus life is changing in ways that would have been impossible to imagine even a decade ago. "We have video and data and texting and sharing information and collaboration, and we have viruses and worms and Trojans being passed back and forth. It's a highly infectious environment, like the club scene in the 1980s," says Bill McGee, security solutions manager for Cisco Systems, another company offering network security solutions to colleges and universities. "You want collaboration to happen, but it has to be safe."

Students aren't the only ones who want easy access to the network from a variety of devices. Faculty, too, need anytime, anywhere access. A professor might want to be able to grade papers on the train using his smart phone and then repost them back to student mailboxes, or sit in a coffee shop and log on to the campus network wirelessly to work on lesson plans.

Hypothetically, there could be a student at the coffee shop using his computer to pose as a wireless access point, and the faculty member might log in via that person rather than via the coffee shop's network. Then, says McGee, the student could "sit in the middle of the coffeehouse, watching all the traffic that's flowing through. [Colleges] need to take appropriate countermeasures against that kind of attack."

Campuses that have graduate-level offerings pose an even greater security challenge. Some of the biggest recent security threats to colleges and universities have come from graduate student labs, says McGee. And schools with hospitals attached have had patient information inadvertently made available because there is an overlap between patients and students.

Technology managers know that cyber crime is a very real threat. In fact, $202 million is lost to cyber crime every year in the U.S. alone, according to Cisco.

To meet the demands of anytime, anywhere access and allow for the open exchange of information, while simultaneously protecting users and the network, an institution needs to have a robust technology infrastructure that takes a layered approach to security, experts say.

What a layered approach might look like

Layered security refers to the combination of security products, at different levels of the network, that can strike a balance between strong network security and open network access for all users—and finding the right balance between these objectives will vary from institution to institution.

"One of the biggest things we're seeing in education is that, in terms of security, if something doesn't look right, [campus officials] shut it down," says Michael Rothschild, solutions marketing director for Juniper. "And one of the biggest issues with that approach, especially in a university setting, is freedom of speech. Someone might be doing something totally normal, but if it's a questionable activity, it gets shut down. It's like using a hammer to kill a fly."

By taking a layered approach, he explains, colleges and universities can look at risks on a more granular level, which allows them to be more specific in terms of how they handle each individual threat.

A typical layered approach can be broken down into four main categories of service:

- *Access Control and Authentication*

Access control refers to the ability to limit access to different types of content or activities. For example, if a computer lab is only to be used for research or science and math, and people are using it for video games, a local firewall can stop people from using the lab for that activity.

Firewalls also can help protect against "Denial of Service" (DoS) attacks, in which a malicious attacker can flood a network with incoming packets of information to try to bring it down.

"At this level [of security], you're forced to authenticate," says McGee.

The security solutions put into place can determine who a user is, what device the person is using, and the

Network Security, page 18

Top-notch security a must to remain in compliance, gain grants

Investing in procedures, training, and equipment that can make networks more secure is well worth the expense for higher-education institutions, and not only for the savings to bank accounts—and reputations—that can result from avoiding costly security breaches.

"In a time of increased national security concerns, pressure is mounting for colleges to gain better control of their computer networks—or risk losing federal grant money for research," Michael A. McRobbie, vice president of information technology for the Indiana University system, recently told an audience at the annual meeting of the higher-ed technology advocacy group EDUCAUSE.

James Webb, chief information officer at West Texas A&M University, agrees. For example, he says, "if your institution deals with credit cards—and almost all of us do—the Payment Card Industry now requires quarterly scans by a PCI-approved scanning vendor. We [also] have Texas Administrative Code 202 at the state level, which requires institutions of higher education to adhere to well-defined information security standards. TAC 202 also requires vulnerability testing to be conducted on an annual basis."

Recent additions to TAC 202 now require an independent review of an institution's information security program.

"The penalty for not keeping up with such requirements could include financial penalties or loss of funding," he says. —J.N.

How four institutions manage security threats

IT managers at Stanford University were concerned. As security threats to colleges and universities increased, Stanford needed to keep private matters private—but at the same time, the university's IT staff wanted to ensure that its wealth of information resources remained widely available to students, faculty, and researchers.

Yet, each academic department and school was responsible for its own network security measures, leaving this vital layer of protection an "incomplete patchwork," school officials explained. The university needed an organization-wide firewall service that could accommodate a highly decentralized environment.

Stanford divides its campus network into eight operational zones, with each zone partitioned into multiple virtual firewall or security zones. Each security zone needed a unique set of security policies, virtual private network (VPN) access controls, and administrators.

To solve this challenge, Stanford deployed more than 20 Juniper Networks NetScreen-5000 Security Systems at the network perimeter and data center to protect the academic, administrative, and residential networks against malicious attacks and intrusions. Stanford now offers a baseline firewall service at no cost to all departments, and additional firewall services are available by request.

The Juniper Networks firewalls are deployed in redundant pairs to maximize resiliency and uptime. Full-mesh configurations allow for redundant physical paths, which also maximizes resiliency and helps the university protect its IT resources in the event of a campus emergency.

The firewalls reduced Stanford's risk exposure and improved security compliance by offering a consistent level of firewall protection that meets the individual needs of its departments—and Stanford IT executives say the virtualized security service was deployed quickly and without disruption to IT operations.

Stanford integrated the NetScreen-5000 line of firewalls with its NetDB database, which offers a way of registering a unique name and IP address for each networked computer, to create a decentralized, self-service model in which firewall policies can be implemented hourly. The university also gained operational efficiencies by standardizing on Juniper Networks firewalls, as its IT staff no longer must manage and maintain firewalls from multiple vendors.

Northwestern University also constructs its security network in layers. "Juniper supplies our campus network border routers—the ones that connect us to the outside world, other research institutions and networks," says Julian Y. Koh, Northwestern's manager of network transport, telecommunications, and network services. "That's the first place you want to start applying security filters."

The university also uses Juniper security at the firewall layer. "We have dedicated firewall appliances in front of our data center to protect the data center and enterprise applications from attack, not just from the outside world but also from anyone on campus," Koh says. His department gives schools within the university the option to contract with IT for their local firewall services. If a given department or school has a small number of machines to protect, IT might deploy a low-end firewall. If a school has greater demands, such as the need to protect a high-speed computing cluster or a larger number of machines, Koh can ramp up the capabilities to meet its needs.

In addition, Northwestern uses Juniper for secure remote access. The university deploys Juniper SSL VPN technology to provide secure access to sensitive data and restricted applications. With this technology in place, says Koh, it has been easy to define various roles and give users different levels of access depending on who they are.

The layered approach has been successful, as have been Juniper's products. Northwestern first began using Juniper close to 10 years ago but recently replaced its original routers with the same kind from Juniper. "That shows our confidence in their function," Koh says.

Securing distance education

The University of Central Florida, with 21 regional delivery sites, has more than 23,000 students taking online courses. UCF's data network has become a critical resource that supports education, research, administrative services, and campus communications—particularly for those students engaged in distance education.

"The network is a part of how we teach and how we do business," says John C. Hitt, UCF president. Maximum network reliability, then, is mandatory—and security issues must not be allowed to jeopardize the network that employees and students depend on every day, IT staff knew.

Yet, network security threats were costing the university money and time. The steady increase in viruses, DoS attacks, and similar threats made it clear that improved network security and monitoring were required. UCF decided to implement a security solution that included:

- Perimeter security with Cisco PIX security appliances and Cisco Catalyst 6500 Series service modules;
- Intrusion protection with Cisco IDS sensors and the Cisco Catalyst 6500 Series IDS Service Module, to identify and classify known and unknown threats; and
- Secure wireless and VPN connectivity using Cisco VPN 3030 concentrators to establish secure connections across TCP/IP networks, including the internet.

Now, the university's computer systems are securely protected from both internal and external risks, campus officials say. For example, the IT team was able to quickly respond to the Nimda worm in 2001, preventing it from spreading across the UCF network. Cisco technology enabled the team to track the affected machines and immediately remove them from the network, UCF officials say.

Quinnipiac University, in Hamden, Conn., has a much smaller student body but faces the same challenges, needing to walk the tightrope between giving users easy access to information and the constraints of government and industry privacy and protection standards.

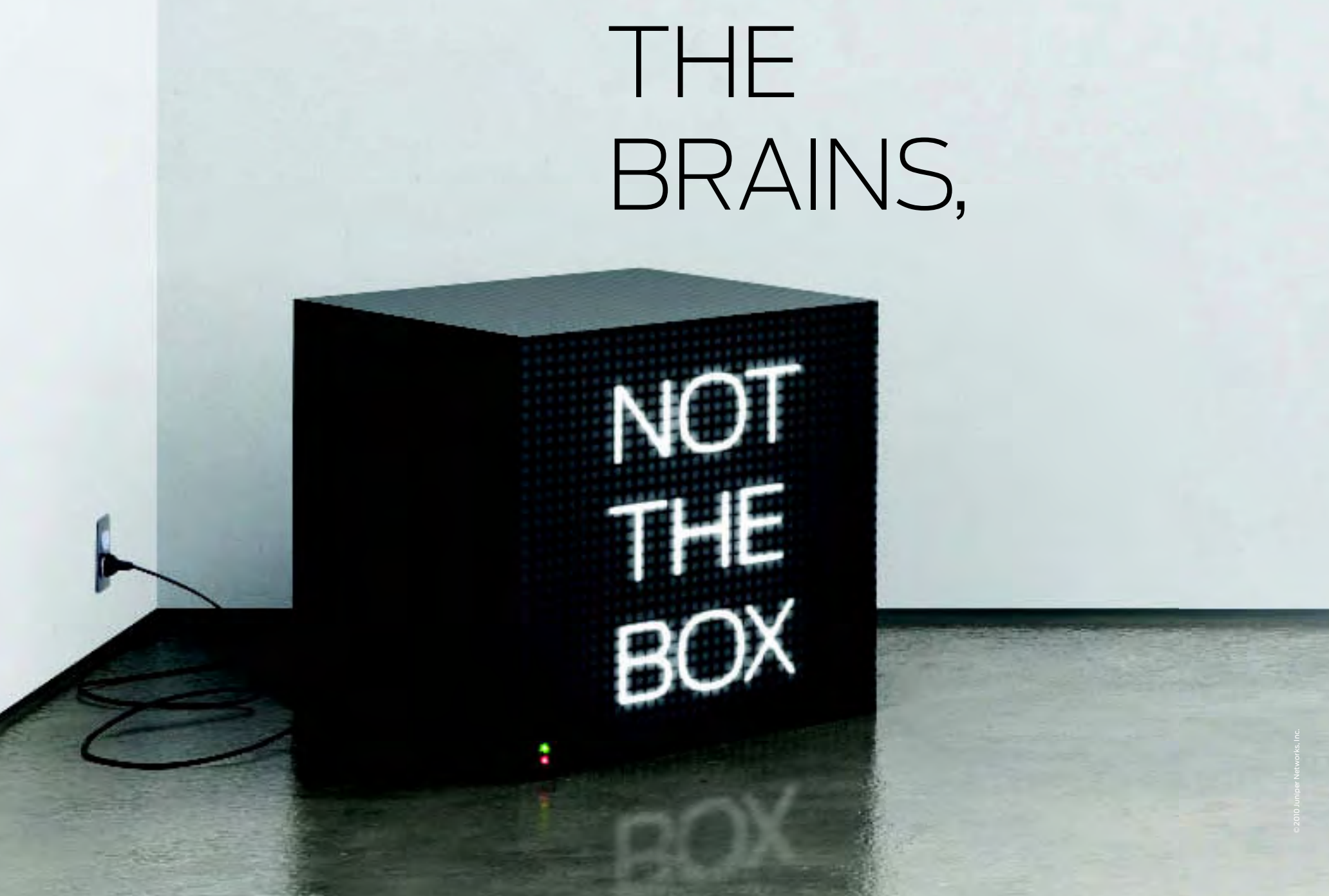
For instance, the Higher Education Act of 1965—recently reauthorized with strict rules regarding copyright—and the Family Educational Rights and Privacy Act protect sensitive student information. Quinnipiac wanted to make sure it was compliant, so Brian Kelly, information security and network operations director for the university, knew he and his team needed to redesign their enterprise security strategy.

The first step was to gain a clear, real-time view of security issues across the network, via a sophisticated intrusion prevention system (IPS) from Hewlett-Packard. Kelly uses the IPS to aggregate and analyze logs from various watch points throughout the enterprise. Drawing information from a single database, rather than going from device to device to pore over system logs, has enabled Quinnipiac's IT team to accomplish more comprehensive monitoring, auditing, reporting, and event mitigation.

"Before our IPS, we were using a series of homegrown utilities to try to aggregate and sift through system logs," Kelly says. "But we don't have a lot of full-time employees, so we either missed things or wasted valuable staff resources."

Now, the team has instant access, via a single pane of glass, to critical security data, including network usage and possible threats. Team members can more easily deploy, update, and enforce access and configuration policies. And automating these tasks and giving appropriate personnel customized information frees up IT resources to be used on other, more strategic projects. It also empowers users to make better, faster decisions about data and network protection, Kelly says. —J.N.

IN THE
NEW
NETWORK
IT'S ALL
ABOUT
THE
BRAINS,



The challenges raised by the massive increase in networked devices used by students and faculty and their escalating bandwidth demands will not be solved by more hardware, but by a radical rethink in the way networks work.

It calls for a whole new philosophy and that's where Junos® comes in.

THE SOLUTION

A revolutionary combination of software, silicon and systems architecture. It's how to make the box smarter. And it's only from Juniper Networks.

Junos is more than an operating system. It's the open-standards, integrated and familial approach to network design at the heart of Juniper routers, switches and security devices. It's a game changer because it brings stability to an environment that has been rife with interoperability issues. Because it creates a platform for third-party innovation and development, and because, in concert with the Junos One family of processors, it enables a new network architecture that is simpler and more powerful than anything before it.

The result is open, interoperable software-powered networking that is scalable, secure and automated.

The new network is here.
And it could be running your campus.

juniper® NETWORKS

TheNewNetworkIsHere.com

Network Security...

continued from page 14

level of access that he or she has been granted to various parts of the network. They also can check a user's device to make sure there are no viruses and that it has the required antivirus software turned on. If the user's device does not meet those requirements, the user can be routed to a place where he or she can find an explanation of how to become compliant by downloading the appropriate software. Once the user has done this, he or she once again can log onto the network, this time successfully.

Firewall appliances, such as Juniper's SRX Security Services Gateways, also can allow higher-education institutions to create distinct "virtual" network segments, and manage which users have access to those segments. Higher-ed institutions can separate graduate students from undergrads, engineering students from liberal arts students, and different schools or departments within the university from each other.

"Before, engineering would build one network, and liberal arts would build another. But now, [institutions] can build [a single] network and virtualize it; engineering would be a virtualized portion of the network, liberal arts would be another. They can scale it very well, and there's tremendous cost benefits," McGee says.

By defining virtual security zones on a firewall, the campus network is logically divided into separate service segments, each with its own rules. This allows educational organizations to create, manage, and enforce rules in which only users from a certain department, for example, can access that department's applications and data.

Centralized management is important to creating a layered approach to security, says Juniper's Herrera. "Firewalls can get very complicated to manage, so the ability to manage at scale, and with a centralized management console so you can see [permissions data] across the organization, is important," he explains.

A centralized access policy manager resides on the local area network (LAN) itself, to ensure that only authorized users can gain access to network destinations. It protects the campus network at the "data link layer"—the point of internet entry, or Layer 2 in the Open Systems Interconnection (OSI) model of network architecture—by identifying and authenticating each LAN user before the network provides the user with an IP address.

• *Intrusion Prevention*

The next layer of protection in the typical layered security model involves application-level protection technologies that monitor network traffic and dynamically analyze it for signs of attacks or intrusions. These devices search for hidden security threats inside common applications such as eMail and instant messaging. Intrusion prevention system (IPS) devices examine control and data fields within the application flow to verify that the actions are allowed by your security policy and do not represent a threat to end systems. They can identify content out of the norm or content that represents a known attack or exploit from worms, Trojans, spyware, and other threats.

IPS devices can examine the subject field, attachment name, or attachment type within eMail traffic to detect characteristics of known viruses, for example.

Solutions such as Juniper Networks' IDP Series Intrusion Detection and Prevention Appliances detect both known and unknown application-layer threats within network traffic and eliminate those threats in real time. The IDP Series also detects the use of unauthorized applications such as instant messengers or file sharing.

Universities could lose their federal student loan status if they don't comply with laws governing copyrighted material on the web, says James Webb, chief information officer at West Texas A&M University. His team put a system into place preventing illegal peer-to-peer file-sharing traffic in which copyrighted material such as movies or music is exchanged.

If the university's IPS device detects such activity, the students are directed to a site explaining that what they are doing is illegal, and they must agree that they won't attempt to do it again. Each time they attempt to exchange such material, they receive 10 points, and if they rack up 40 points, they are banned from the network until they go through student judicial affairs and get clearance to log back on. "That cuts down on illegal peer-to-peer traffic," says Webb.

• *Unified Threat Management*

Another layer of security involves file-level protection, which gives the ability to extract individual files within network traffic and inspect them to detect malware, including viruses, worms, or Trojans.

A common technology for file-level protection in a network is an antivirus gateway. Antivirus systems typically scan files in eMail and web traffic, mainly inspecting communication from servers to clients. Viruses are aimed at damaging or compromising end-user systems, but they use various eMail and web servers to propagate. Consequently, it's important to detect viruses while they are being uploaded to, or downloaded from, servers.

"Someone might be doing something totally normal, but if it's a questionable activity, it gets shut down. It's like using a hammer to kill a fly."

— Michael Rothschild, solutions marketing director for Juniper Networks

Antivirus systems can search for virus signatures—a unique string of bytes that identifies a virus—and zap the virus from the file. According to Juniper, most antivirus scanning systems catch not only the initial virus but also many of its variants, because the signature code usually remains intact. Gateway antivirus systems scan files that are embedded in network traffic, including files in HTTP and eMail traffic, sent as attachments. If an infected file is detected, a gateway antivirus system removes it from the traffic, so that it does not affect other users.

• *Encrypted Communications*

A fourth layer of security involves setting up secure connections between locations that encrypt transmissions using VPN technology when the transmissions are running across untrusted media, such as the internet. There are multiple kinds of VPN solutions from which to choose, and no single type of solution is the right option for every situation.

Internet Protocol Security (IPsec), for instance, is a set of protocols for securing IP communications by authenticating and encrypting each IP packet of a communication session. IPsec is an end-to-end security technique that operates in the internet layer of the OSI networking model. It can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

Other internet security protocols operate in the upper layers of the networking model. Secure Sockets Layer (SSL) and Transport Layer Security (TLS), for example, encrypt data at the application layer. Several versions of these protocols are in widespread use in applications such as web browsing, eMail, and voice over IP.

For fixed remote campus locations, Juniper suggests that IPsec is the preferred method for deploying VPNs. IPsec can operate with low latency for applications that require high performance. Once they are configured and in place for fixed locations, they typically do not need to be reconfigured and usually can operate without manual intervention.

For the teleworker and mobile campus population, a better alternative might be to use SSL VPNs. Because the SSL VPN uses technology embedded in all standard web browsers, it uses a clientless platform and requires little or no manual configuration on behalf of the user or changes to internal servers. This makes VPN access seamless to the remote user.

"When you have all these different layers of access control with a network access solution, you're able to get very granular and very specific in terms of what's allowed and not allowed," says Herrera. And you can ensure that, when a threat occurs, it is not only stopped, but is also reported, so that IT staff can know where potential problems lie.

Choosing the right security solution

When choosing a next-generation security solution, it's important to pick a solution that can work with whatever networking equipment and vendors your school is already using.

In times past, when IT managers found a solution that did not work with what they already had, the notion of "rip and replace" was a suitable action: They simply ripped everything out and started over. Today, with far less money available to universities, the notion of augmentation—that is, adding on to what already exists and making the technologies work together—is far more viable.

IT managers must ask what kind of disruption a new security technology will cause, says Rothschild. Juniper's solutions are able to operate across multiple vendors' equipment: If a school already uses someone else's firewalls, "[with] our intrusion prevention system, we can correlate multiple feeds across these different products to root out stealthy activity," Rothschild says.

Whatever solution or combination of solutions you choose, addressing the new and growing variety of network security risks while increasing your institution's flexibility and capacity to innovate is a delicate balancing act—one that requires your technology infrastructure to be robust enough to handle the challenge.

"In order to have good security, it is very important that people know how their networks are set up, and what normal behaviors are, so they can notice anomalies and trends," says Koh. "Choosing vendors whose equipment and systems can give you visibility into those trends and metrics is one of the most important things to consider when choosing whom to work with."

Jennifer Nastu is a freelance writer who frequently covers technology in education.

Network Security Glossary of Terms

ACL (access control list): A method of keeping in check the internet traffic that attempts to flow through a given hub, router, firewall, or similar device. Access control is often accomplished by creating a list specifying the IP addresses and/or ports from which permitted traffic can come. The device stops any traffic coming from IP addresses or ports not on the ACL.

AH (authentication header): An IPsec header used to verify that the contents of a packet have not been modified while the packet was in transit.

Alias: A shortcut that enables a user to identify a group of hosts, networks, or users under one name. Aliases are used to speed user authentication and service configuration. For example, in configuring a firewall, a user can set up the alias "Law School" to include the IP addresses of every network user in a university's law school.

Auto-partitioning: A feature on some network devices that isolates a node within the workgroup when the node becomes disabled, so as not to affect the entire network or group.

Block cipher: A procedure that translates plain text into coded text, operating on blocks of plain text of a fixed size (usually 64 bits). Every block is padded out to be the same size, making the encrypted message harder to guess.

Blocked port: A security measure in which a specific port is disabled, stopping users outside the firewall from gaining access to the network through that port. The ports commonly blocked by network administrators are the ports most commonly used in attacks.

Botnet: A collection of computers that are infected with small bits of code (bots) that allow a remote computer to control some or all of the functions of the infected machines. The botmaster who controls the infected computers has the ability to manipulate them individually, or collectively as bot armies that act in concert. Botnets are typically used for disreputable purposes, such as Denial of Service attacks, click fraud, and spam.

Certificate: An electronic document attached to someone's public key by a trusted third party, which attests that the public key belongs to a legitimate owner and has not been compromised. Certificates are intended to help you verify that a file or message actually comes from the entity it claims to come from.

Certificate authority (CA): A trusted third party (TTP) who verifies the identity of a person or entity, then issues digital certificates vouching that various attributes have a valid association with that entity.

CHAP (Challenge Handshake Authentication Protocol): A type of authentication where the person logging in uses secret information and some special mathematical operations to come up with a number value. The server he or she is logging into knows the same secret value and performs the same mathematical operations. If the results match, the person is authorized to access the server. One of the numbers in the mathematical operation is changed after every login, to protect against an intruder secretly copying a valid authentication session and replaying it later to log in.

Cross-site scripting: An attack performed through web browsers, taking advantage of poorly written web applications. Cross-site scripting attacks can take many forms. One common form is for an attacker to trick a user into clicking on a specially crafted, malicious hyperlink. The link appears to lead to an innocent site, but the site is actually the attacker's and includes embedded scripts. What the script does is up to the attacker; commonly, it collects data the victim might enter, such as a credit card number or password.

CVE-compatible: Common Vulnerabilities and Exposures (CVE) is a list of standardized names for vulnerabilities and other information security exposures, whose aim is to standardize the names for all publicly known vulnerabilities and security exposures. "CVE-compatible" means that a tool, web site, database, or service uses CVE names in a way that allows it to cross-link with other repositories that use CVE names.

DES (Data Encryption Standard): A commonly used encryption algorithm that encrypts data using a key of 56 bits, which is considered fairly weak given the speed and power of modern computers.

Dictionary attack: An attempt to guess a password by systematically trying every word in a dictionary as the password. This attack is usually automated, using a dictionary of the hacker's choosing, which might include both ordinary words and jargon, names, and slang.

DMZ (Demilitarized Zone): A partially protected zone on a network, not exposed to the full fury of the internet, but not fully behind the firewall. This technique is typically used on parts of the network that must remain open to the public (such as a web server) but must also access trusted resources (such as a database). The point is to allow the inside firewall component, guarding the trusted resources, to make certain assumptions about the impossibility of outsiders forging DMZ addresses.

DNS spoofing: An attack in which a hacker intercepts your system's requests to a DNS server in order to issue false responses as though they came from the real DNS server. Using this technique, an attacker can convince your system that an existing web page does not exist, or respond to requests that should lead to a legitimate web site, with the IP address of a malicious web site.

Domain name hijacking: An attack technique where the attacker takes over a domain by first blocking access to the victim domain's DNS server, then putting up a malicious server in its place.

Failover: A configuration that allows another machine to take over in the event of a stoppage in the first machine, thus allowing normal use to return or continue.

Fail-shut mode: A condition in which a firewall blocks all incoming and outgoing network traffic in the event of a firewall failure. This is the opposite of fail-open mode, in which a firewall crash opens all traffic in both directions.

IP spoofing: The act of inserting a false (but ordinary-seeming) sender IP address into the "From" field of an internet transmission's header in order to hide the actual origin of the transmission. There are few, if any, legitimate reasons to perform IP spoofing; the technique is usually one aspect of an attack.

Packet filtering: Controlling access to a network by analyzing the headers of incoming and outgoing packets, and letting them pass or halting them based on rules created by a network administrator. A packet filter allows or denies packets depending on where they are going, from whom they are sent, or what port they use. Packet filtering is one technique, among many, for implementing security firewalls.

PKI (Public Key Infrastructure): A system of digital certificates, Certificate Authorities, and other registration authorities that verify the validity of each party involved in an internet transaction. The intent is to establish a trusted relationship between the parties. PKI is necessary for certificate-based Virtual Private Networks.

Probe: A type of hacking attempt characterized by repetitious, sequential access attempts. For example, a hacker might try to probe a series of ports in search of one that is open, or one might probe a range of IP addresses in search of a responsive computer.

Public key cryptography: Cryptography in which a public and private key pair is used, encrypting the data at the sender's end and decrypting it at the receiver's end. Because the data are encrypted while they travel the public internet, no additional security is needed—the data can safely use public networks without loss of confidentiality.

Session hijacking: An intrusion technique whereby a hacker sends a command to an already existing connection between two machines, in order to wrest control of the connection away from the machine that initiated it. The hacker's goal is to gain access to a server while bypassing normal authentication measures.

Session key: The secret (symmetric) key used to encrypt each set of data on a transaction basis. A different session key is used for each communication session.

Social engineering attack: An attack that does not depend on technology as much as it depends upon tricking or persuading an individual to divulge privileged information to the attacker, usually unknowingly.

Spoofing: Altering data packets to falsely identify the originating computer. Spoofing is generally used when a hacker wants to make it difficult to trace where the attacks are coming from.

SSID (Service Set Identifier): A unique string, up to 32 characters, that serves as the name of a wireless local area network (WLAN). Because a SSID differentiates one network from another, multiple wireless networks can function even when their ranges overlap. In an open network, the access point broadcasts the SSID. You can configure your wireless access point (WAP) not to broadcast the SSID, so that users trying to join the network must already know the network name.

SSL (Secure Sockets Layer): A protocol for transmitting private documents over the internet, often used by eCommerce sites (among others). SSL works by using a private key to encrypt data transferred over an SSL connection.

Triple-DES (3DES): A cryptographic algorithm using three keys (rather than one or two). Triple DES is simply another mode of DES operation, where the DES algorithm is applied three times on the data to be encrypted, using a different key each time.

(Source: WatchGuard)

HOW TO SECURE VAPOR.

CLOUD-READY SECURITY

The open, shared resource of the cloud offers opportunity for colleges and universities everywhere. Securing the cloud is the #1 challenge in adopting this new approach to networking.

On its surface, putting your data “in the cloud” doesn’t exactly sound safe. The solution thus far has been to fall back on the old “castle and moat” approach—protect the perimeter at all costs. But this is cloud computing. The whole idea is about letting students and faculty in—the data flowing freely and efficiently. So how do you secure a perimeter that needs to stay porous?

Juniper has pioneered a virtualized security services platform specifically designed for the shared environment of the cloud. Rather than throwing up a wall, this approach protects data flows on an individual basis, on every layer. It’s a holistic and virtual solution, not unlike the cloud itself. The new network is here and it’s securing the cloud.

TheNewNetworkIsHere.com

Juniper NETWORKS