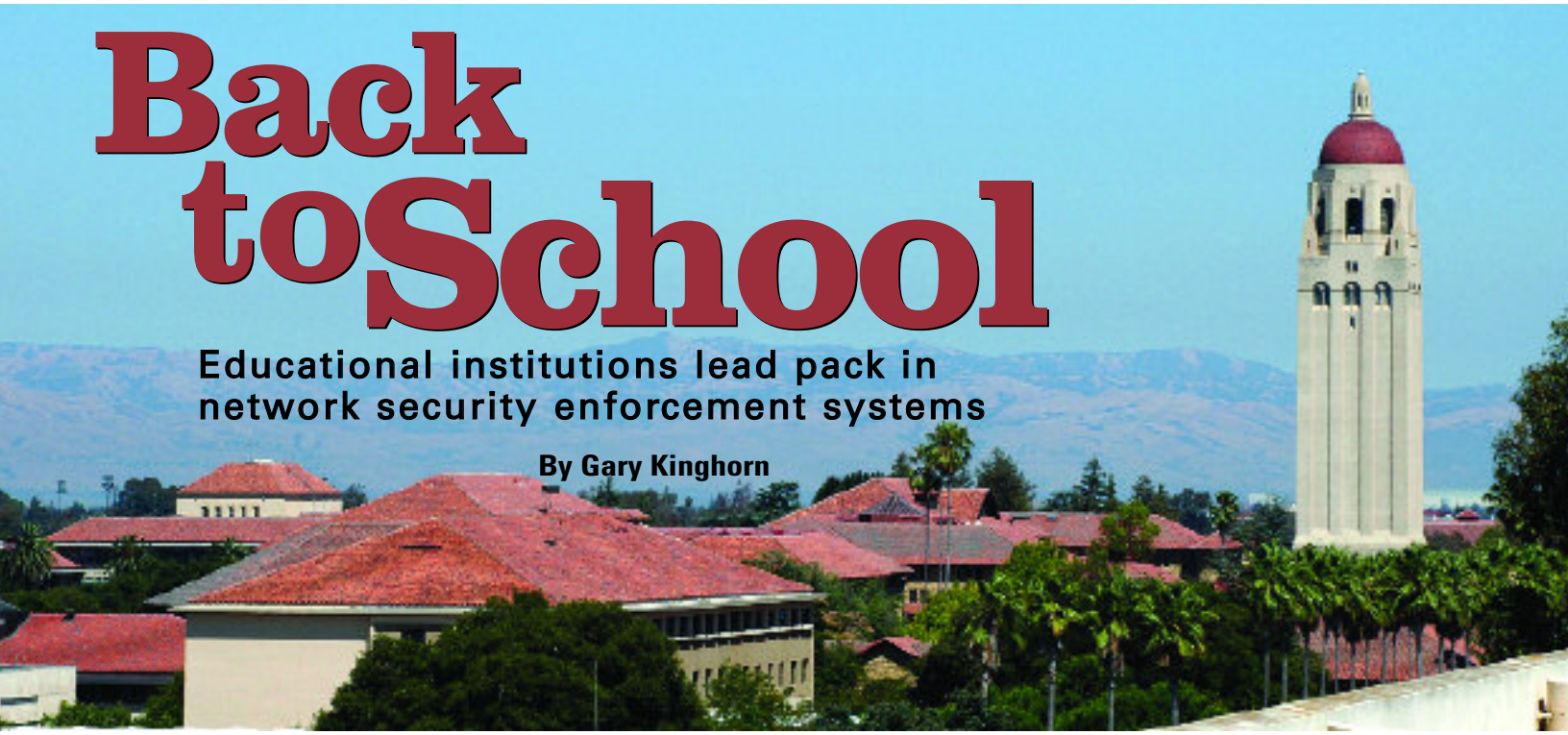
Back to School



Educational institutions lead pack in network security enforcement systems

By Gary Kinghorn

Educational institutions don't often come to mind when people think about organizations with cutting-edge network security devices. However, these institutions face the daunting task of keeping the networks secure while allowing tens of thousands of students and faculty to bring their own PCs onto the network. They also have to account for a user base that changes by many users on an annual basis.

Trying to create, manage and enforce a security policy has to take into account many untrusted users and unmanaged endpoints, and the frequency of change is becoming increasingly normal in more and more organizations. And while the typical university or school district may not have the risk of financial loss due to compromised intellectual property—like a large drug manufacturer or the sensitive customer data of a major financial institution—they do have mission-critical student and HR data that has to be protected. For fledgling hackers, there is no more prized target than their own school's grade repository.

RETHINKING OPEN NETWORKS

The Upper Canada District School Board (UCDSB) is taking on these challenges by rethinking how LAN security should be implemented and what constitutes best practices in designing "open" networks. UCDSB is located in northern Ontario and consists of more than 35,000 networked users at 120 rural elementary and secondary schools spread over a wide geography. Many students bring their own mobile devices to the various campuses, including PDAs and laptops. According to Jeremy Hobbs, CIO of UCDSB, many of the virus and worm outbreaks the district experienced in past years are directly attributed to these external mobile systems.

The challenge of securing a LAN against a dissolving perimeter, external endpoints and untrusted users is not new, but many of the best practices in addressing the problem are changing rapidly. Organizations can no longer rely on perimeter security devices and traditional gateways, like VPN and wireless access points. Access is emanating from many more locations, including conference rooms, and there are few policy enforcement mechanisms within an organization. What have leading organizations been doing to protect their network resources in light of this?

Network access control, as defined in various standards supported by Cisco, Microsoft, Juniper and others, has received a great deal of enthusiasm for its ability to provide access to the enterprise network by an unmanaged endpoint contingent on systems conforming to the access policy of an organization. Such policies typically include proper configuration of the system software, as well as anti-virus and anti-spyware programs. NAC, however, has recently begun to slide down the backside of Gartner's hype cycle and into the trough of disillusionment. A recent Forrester research report essentially declared NAC was unlikely to deliver long-term benefits to early adopters and was likely to be supplanted by more comprehensive approaches within the next few years. NAC is a reasonable first step in providing security inherent to the

IT Security

LAN, but it was never intended to provide full defense against untrusted systems.

"We had one major criticism of NAC after we considered it," Hobbs said. "Network access is based solely on the endpoint authorization check, and an all-or-nothing access to resources is determined from that. Once users and systems are allowed onto the network, the burden is still on our network security staff to restrict access by the external users to sensitive data and resources, as well as to stop the zero-day and targeted attacks that the desktop anti-virus software was not designed to detect."

Some enterprises elect to deploy some form of intrusion prevention system, such as a host-based IDS or an in-line IPS, as well as an NAC solution.

NAC ALTERNATIVES

As one alternative to NAC, access control policies are often enforced internally through firewalls and LAN segmentation, as well as directly on the application or server endpoint. There are a couple of problems traditional approaches include, however. First, implementing access control through firewalls and LAN segmentation is tedious and expensive to modify as users and policies change. Because firewalls look at source and destination IP addresses, policies have to be designed around a system's location, which is becoming less and less certain in many network environments. As a result, rarely do the intended access policies correspond smoothly to the LAN implementation and enforcement mechanisms. Trying to enforce access control policies on the application or server also is flawed because it does not prevent brute force or distributed attacks to that system or stop denial of service attacks aimed at that server.

"Where we saw similar projects to ours fail, there was probably too much emphasis on solving the network security problems with desktop software," Hobbs said. "Plus, we tend to be leary of client-side software from a security perspective. Whether an anti-virus program, host-based IDS, NAC client or the operating system itself, it will always have vulnerabilities and be capable of being taken over by rogue software. It's just not a foolproof way to defend the LAN. Besides, we just don't manage all of the endpoints connecting to our network now. Requiring them to have the right policy-compliant software intact is probably a futile endeavor. Confining enforcement to the client endpoint is like saying to outsiders, 'We don't trust you, so please do a good job of policing yourself.'

"The goal is to defend the network against the systems and users you don't trust but have to allow in. The onus of enforcing the network security policy has to fall back on the network itself."

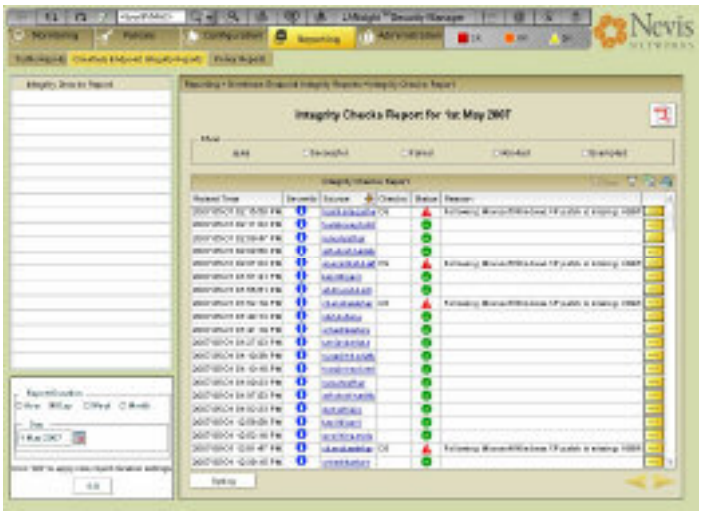
THINKING OUTSIDE THE BAND

A slightly more sophisticated approach is to enforce network security policies in an out-of-band appliance, which at least moves the security functions off the desktop and server system and into the network. Out-of-band solutions provide no enforcement capability at all, though, because they only look at a mirror copy of the traffic and can't effect any remediation on malware and malicious user packets traversing the in-line traffic flow. The debate over an out-of-band solution versus an in-line security approach—where the security enforcement appliance is placed directly in the flow of traffic—has had strong proponents on both sides. The arguments are now falling firmly in favor of an in-line approach due to the increasing demand for post-connect security enforcement and growing numbers of successful deployments.

Jeremy Hobbs, UCDSB's chief information officer, and staff show off the Nevis LANenforcer and LANsight systems that protect the network from untrusted endpoints, users and malicious code.

"We didn't spend much time evaluating out-of-band solutions," Hobbs said. "A solution has to be in-line to enforce policy, quarantine worm packets or filter out unauthorized user access attempts, rather than just in a logging or advisory mode, as an out-of-band solution could do. We were looking for an active enforcement and remediation approach."

The hesitation to deploy in-line has been overcome through advances in custom silicon, which dramatically raises performance to provide robust security services without slowing network traffic. It also has the ability to apply extremely precise remediation. An in-line intrusion prevention system responds by shutting down a network port or service, which greatly impacts user productivity or business activity. However, state-of-the-art solutions now have the ability to deeply inspect packets at peak network speeds, filtering out



The Nevis LANsight management console displays top attacks and threats throughout the network in this report.

specifically only the worm packets, and letting all other users and legitimate business activity proceed unimpeded. This dramatically reduces the risk of adverse business consequences and allows the appliance to take a proactive and immediate remediation response.

BALANCING ACT

When confronted with the challenges, UCDSB knew the solution had to meet certain criteria to comply with external systems and user access without being a business risk or performance bottleneck. From the beginning, officials knew the district needed an in-line appliance that enforces the access control policies already in place. This ruled out a number of out-of-band solutions. But officials also were looking for more than just an NAC endpoint validation solution.

"UCDSB was looking for an identity-driven infrastructure that would not only authorize users to connect to the network, but would control behavior and defend against rogue threats continuously throughout the user session in the post-connect phase," Hobbs said. "An enforcement solution built around user identities is important for us because that's how policies are built and managed—around user and group names—not physical machine identifiers, many of which we have almost no visibility to. If we were going to effectively maintain the network policy, the enforcement of both network access and access to resources had to be linked to user identities or defined groups."

Like any networked business environment, Hobbs has to continually balance security issues with enabling access, productivity and business continuity. An outbreak of a virus is almost more tolerable than shutting down access to a critical server due to a false alarm.

"The fact that the remediation of the Nevis device is transparent to the user is a huge factor in being able to confidently deploy an in-line appliance, while at the same time putting the enforcement in the network where we can manage it, rather than on the untrusted endpoint itself," Hobbs said.

At the end of the project, UCDSB has essentially layered a policy enforcement engine into their network that enforces access control to mission-critical resources based on user identities. It also upholds endpoint access policies by authenticating users and ensuring the client's software configuration and health. Security policies are centrally managed or pulled from existing policy repositories and enforced throughout the school district's LAN. Policy management is simplified, remediation is more efficient and the network is safe, no matter what the students or their teachers decide to try next.

Gary Kinghorn *is the senior product marketing manager at Nevis Networks. He can be reached at gkinghorn@nevisnetworks.com.*

www.nevisnetworks.com

Nevis Networks, Inc.
295 Bernardo Ave., Suite 100
Mountain View, CA 94043
(650) 254-2500

Nevis Networks India
C301 Pune IT Park
Bhau Patil Marg
34 Aundh Road
Pune 411020, India
Tel: +91 98450-05047

Nevis Networks International HQ
Delegate House
30 Hart Street
Henley on Thames, UK RG9 2AL
Tel: +44 1491 635 339