REAL TIME NETWORK PROTECTION FOR EDUCATIONAL INSTITUTIONS

White Paper

February, 2003

Abstract

Along with the tremendous educational benefits brought about by the Internet have come increasingly difficult network security threats and challenges. To begin with, network threats have changed from identity-based threats to content-based ones, putting enormous pressure on network security assets to try to adapt. Compounding matters is the growing emphasis on “real time” communication and access to information, which forces these network security assets to work even faster to find malicious content before it can do its harm. Conventional network security systems – which are just a collection of mostly software-based point solutions cobbled together into an ad hoc “system” – have not been able to keep up with the need for “real time” protection. By contrast, Fortinet’s Antivirus Firewalls address all the network security needs of educational institutions. Fortinet’s ASIC-powered Antivirus Firewalls scan email and web content at the network edge and in real time – protecting the educational network from viruses, worms and other inappropriate and malicious content before it can enter the network. In addition to real time antivirus and content filtering protection, Fortinet’s Antivirus Firewalls combine firewall, VPN and IDS functionality in one easy to install, maintain and update unit.
Contents

The Changing Demands on Educational Networks .................................................4
   The Changing Nature of Network Threats ................................................................. 4
   Common Threats and Challenges Faced by Educational Institutions ....................... 5
   Challenges and Issues Specific to K-12 ....................................................................... 7
   Challenges and Issues Specific to Higher Education .................................................. 8

Conventional Solutions to Educational Network Security .................................9
   Shortcomings of Conventional Solutions ..................................................................... 10

The Antivirus Firewall Advantage ........................................................................11
   How Fortinet’s Antivirus Firewalls Address The Needs Of Education ........................ 13

For More Information ..............................................................................................14
THE CHANGING DEMANDS ON EDUCATION NETWORKS

The Internet has increased students’ exposure to many valuable and useful sources of information; unfortunately, however, it has also made it easy to access inappropriate or illegal content and to utilize campus networks for non-educational pursuits. Key issues include:

- Access to inappropriate content by young students
- Intrusions into academic record and exam stores
- Utilization of campus networks for illegal content sharing

These issues have placed an enormous strain on all resources that are associated with the health, maintenance or support of campus computing systems and networks. While numerous products are available today that can be used to filter inappropriate content, eliminate viruses and worms, detect network intrusions and prevent access to critical computing assets, the cost of procuring and managing these systems stretches the personnel and budget limitations of the vast majority of educational institutions. What is needed is a new, architecturally different approach to network protection for educational environments that is effective, inexpensive, easy to install and maintain, and consistent with applicable government requirements.

The Changing Nature of Network Threats

For much of the last two decades, the primary threats to networked computing systems were attacks launched by remote hackers who established connections from outside of the private, or trusted network to resources within the private network, and used those connections to compromise private data and programs. The response to these so-called “connection-oriented” attacks was to install network firewalls at the junctures between the private local area network (LAN) and the public wide area network (WAN) - most commonly the Internet. The primary functions of the firewall are to hide the internal structure of the private network from those outside and to validate that traffic traversing the LAN/WAN boundary is from legitimate senders for legitimate purposes - a process that is based primarily on determining that the remote party is trusted and that the nature of the connection is for something allowed, like Web browsing or email, vs. disallowed, such as remote control. More recently, the most damaging and costly attacks do not require sustained connections from outside to inside the private network; rather, so-called “content-based” attacks, such as viruses, worms and Trojans, deploy active agents within the private network that act autonomously – and rapidly. Detecting content-based attacks is much more challenging than connection-based attacks, because the contents of the communication, rather than simply the source and the nature of the application, must be thoroughly analyzed to determine if it contains malicious code. Indeed, most content-based attacks are delivered by ostensibly “trusted” sources such as email messages and Web pages – two types of traffic that are always allowed by firewalls.

To make matters worse, at the same time that threats are becoming more sophisticated and difficult to analyze and detect, our need to access information and our patience with network performance are now categorized in one of two ways: “real time” or “unacceptably slow.” Whereas just a few years ago email seemed lightning fast
compared to “snail mail”, email itself is often too slow now compared to instant Web downloads or instant messaging. For example, 4 of the top 5 online activities in 2002 were “real time” activities - instant messaging, Web surfing or browsing, reading news, and accessing entertainment information.\(^1\) Communication and access to information must increasingly be in real time in order to meet our needs and expectations. This puts an incredible strain on the processing capabilities of current network security solutions, a strain so severe that these current solutions cannot come close to keeping up. What is needed is a fundamentally faster approach that can scale to meet the needs of today’s comprehensive networks and sophisticated threats.

**Common Threats and Challenges Faced by Educational Institutions**

There are several needs, threats and challenges that are (in varying degrees) common to the full spectrum of educational institutions, from primary and secondary schools (K-12) though higher and adult education. These include protection from viruses and worms, secure connectivity between remote locations and the network, protection from inappropriate content and compliance with regulatory norms, maximization of bandwidth and other network resources, protection of administrative resources and students from hackers, ease of maintenance and updating, maximization of performance, and capital and expense budgets. Each is analyzed separately below.

**Protection from Viruses and Worms**

Viruses are malicious executable programs that are embedded within otherwise ‘legitimate’ files. Worms are similar to viruses in form and delivery except they propagate automatically without user intervention. Attacks are increasingly “blended attacks”, morphing the worst characteristics of viruses, worms, and network intrusions in powerful, multifaceted agents. The number of reported incidents of virus and worm attacks has increased dramatically over the past several years, as has the cost of dealing with these attacks. According to one study, the average number of attacks per company increased by 79% from July 1, 2001 to December, 2001 (Source: Riptech, 2002). The cost of recovering from these attacks is skyrocketing as well. Following the much-publicized Nimda attacks, many major corporations went so far as to cut off Internet connectivity for periods ranging from several days to several weeks. The combined costs related to damage and recovery from the Code Red worm approached $2.5 billion, and the related costs for Nimda were $3 billion. Worldwide, damage from malicious attacks in 2001 has been estimated at $12-13 billion (Source: eWeek).

---

\(^1\) Source: UCLA Internet Report – Year Three.
The much-studied Nimda and Code Red attacks and the more recent “Slammer Worm” are examples of the increasingly sophisticated and disabling attacks commonly known as blended threats. Blended threats spread through networks with unprecedented speed by exploiting known vulnerabilities in widely deployed software applications. Even those organizations that maintain host-based antivirus software are successfully attacked, because blended attacks (like Slammer) can bypass conventional antivirus defenses. Even those infections that can be caught by conventional host-based antivirus software can propagate to PCs and servers faster than the antivirus software can be updated (see host-based antivirus discussion under “Conventional Solutions” below). In addition, new vulnerabilities are exposed by the practice of allowing faculty and students to access their personal, Web-based email accounts from within the campus network, effectively bypassing most networks’ server and desktop antivirus defenses.

**Secure Connectivity Between Remote Locations And The Network**

School districts and universities alike can now be found with tens to thousands of users spread out over numerous locations, many of whom utilize virtual private network (VPN) technology to provide fast, secure access to information stored on the network. VPNs use encryption and authentication techniques to ensure the privacy and integrity of data as it traverses the public network. While generally very effective for providing ubiquitous remote access, VPNs have some significant limitations and shortcomings. Most importantly, conventional VPN hardware and software does not scan the content carried within their “secure” tunnels, and as a result VPNs can provide yet another means by which viruses, worms, and other attacks can penetrate the firewall and reach the private network. Without real time scanning of VPN traffic before it enters the network, VPNs can actually represent a threat as opposed to an enhancement to network security.
Maximization Of Network Resources

Some institutions have reported that file-swapping, as popularized by Napster and continued by its progeny Morpheus, Kazaa and Grokster, represents the largest consumer of bandwidth on their networks. While the legality of file swapping can be debated, the tremendous bandwidth it utilizes cannot. A typical MP3 file is about 300-400 kilobits, and DVD movies can run into gigabytes. Downloads of these files consume enormous amounts of bandwidth, and it doesn’t take many such users to bring the entire network to a crawl. Firewall applications can effectively prohibit this sort of activity by preventing students from downloading certain types of files like mp3s, or by blocking the file swapping protocols. Alternatively, traffic management technology can be used to limit the amount of bandwidth that is allocated to these types of applications.

Protection From Hackers

Whether it involves the classic scenario of a student trying to access their records to change a grade, or a “hacktivist” attempting to express their opinion in a very noticeable (and illegal) way, hacking can cause significant damage to a school’s network and can utilize an overwhelming amount of network resources to prevent, identify and remedy. Unfortunately, because they can purposely grant access to the wrong people, through VPNs, old usernames/passwords, stolen identities or other back doors, firewalls alone are not enough. A comprehensive Intrusion Detection System (IDS) can help identify hackers and stop them in their tracks. IDS technology effectively operates as a network’s “sleuth”, constantly watching the network for suspicious activity that indicates an attempt to exploit or overwhelm specific servers and/or applications. An effective IDS system will set off an alarm when such activity fits a known “attack profile” and allows the network administrator to take immediate action to protect the network, either automatically as part of a security policy or manually.

Ease Of Maintenance And Updating

An often overlooked but critically important aspect of any educational network security solution is its ease of use, maintenance and updating. Most educational institutions – regardless of size – have limited budgets for their system/network administration staff. Network protection solutions that require 3, 4, 5 or more distinct applications – each from a different manufacturer with different interfaces, policies and capabilities – results in a daunting and expensive management task that can require extensive staffing.

CHALLENGES AND ISSUES SPECIFIC TO K-12

Access to the Internet by the K-12 student body is regulated and sheltered – by the government, by parents and by the schools themselves – to a much greater degree than in Higher Education. As a result, the challenges and issues specific to K-12 institutions - protection from inappropriate content, and compliance with governmental regulations related to security - are focused on restricting access to certain content.

Governmental Regulations – CIPA

Because the vast majority of public school budgets come from government funding, these schools are subject to the various statutes and regulations enacted by local, state and
federal governments. With respect to K-12 network security, the most important statute is the Children’s Internet Protection Act (CIPA), which was enacted December 21, 2000. Pursuant to CIPA, in order to receive certain “E-Rate” or other federal program funding to purchase computers used to access the Internet, a library or school must have a policy on Internet safety in place. This policy must provide that all computers with Internet access operate with blocking or filtering technology to prevent both adults and minors from accessing child pornography or other inappropriate content, like copyrighted material, pirated songs, videos and movies, or stolen items like calling card numbers or credit card numbers. The unfortunate truth is that pornography and other inappropriate content is readily available to students of all ages; nearly 16 percent of visitors to adult-oriented sites in February 2002 were under the age of 18.² In addition to statutory requirements like CIPA, primary and secondary institutions are concerned with keeping pornography out of the reach of their students for ethical and liability reasons.

Inappropriate content at the K-12 level can largely be kept out of the network by using a Content Filtering (CF) application. These applications prohibit students from accessing or downloading content from websites that contain prohibited URLs (Universal Remote Locators – the technical name for a web site’s “address”) or certain prohibited “keywords.” By not allowing students to view any such prohibited content, CF applications are reasonably effective at keeping such content from students. One drawback of most CF applications, however, is their typically detrimental effect on performance. Because those CF applications that scan each web page’s content for prohibited “keywords” must look at all content on every web page, and are almost always software-based solutions, they can slow network performance. In addition, most CF products or services require a subscription to a periodically updated list of banned URLs, the cost of which can be significant for large student populations.

CHALLENGES AND ISSUES SPECIFIC TO HIGHER EDUCATION

By contrast to the K-12 sector of education, and as a result of its tradition as a haven for thought and expression freedom and leadership, the challenges and issues unique to Higher Education involve addressing the unintended and unwanted byproducts of these freedoms. For example, students can and occasionally will use the school’s network for inappropriate and/or illegal purposes. “File swapping” (e.g. Napster, Morpheus and Kazaa) is a perfect example of such an application that can have a very negative impact on a Higher Education network. University networks are commonly laboratories for new threats, and can also be used to launch attacks on administrative systems.

File Swapping

As mentioned above, file swapping activity may have significant legal ramifications at worst, and at best is a major drain on network resources. One university discovered that peer-to-peer activity had been utilizing 80 percent of the school’s bandwidth, which "essentially brought all applications to a halt."³

² Source: Nielsen/Net Ratings.
While the legal issues are somewhat in the “gray” area, recent developments would suggest the issue may be heating up: the Recording Industry Association of America recently sent a letter to 2300 college presidents, requesting that the schools "inform students of their moral and legal responsibilities to respect the rights of copyright owners" when using the universities' networks.  

**Malicious Constituent Activity**

One alarming trend is the growth of viruses and worms originating from within Higher Education networks. “Smart hackers don’t like to launch…attacks from their own systems. They prefer to take over easily compromised systems at other locations, like universities and poorly defended companies, and use those systems to launch attacks.” This malicious activity can have disastrous effects on the performance of the network and, potentially even more damaging, can subject the institution to extensive liability for damage caused outside of the institution’s network.

**CONVENTIONAL SOLUTIONS TO EDUCATIONAL NETWORK SECURITY**

Whereas before the total number of educational network users – and therefore potential threats – could be counted in the thousands, now the potentially harmful pieces of content number in the billions per minute per network. In other words, the threat has increased by many orders of magnitude from what it was just a few years ago.

How has network security tried to keep up with this changing threat? By rolling out many different “point solutions”, each of which seeks to address a particular component of the whole network security picture. While this approach is certainly better than doing nothing, it has many holes that leave educational networks exposed. Among the many problems with this approach is the fact that these solutions were never designed to work together, and therefore do a poor job interacting and cooperating – leaving the network administrator to figure out how to weave everything into a comprehensive and cohesive network security system.

**Today's Network Security “System”: Point Solutions Cobbled Together**

As figure 1.2 below illustrates, the most typical “conventional approach” to network security in education is not unlike that of its corporate counterpart. In order to provide complete protection, network security “solutions” are collections of individual point solutions cobbled together into a patchwork system, as shown in the following figure:

---

These systems suffer from numerous shortcomings, as described below.

**SHORTCOMINGS OF CONVENTIONAL SOLUTIONS**

**Lack Of Complete Protection**

Given today’s budget realities, few organizations in general, and educational institutions in particular, enjoy the funding required to support the procurement and ongoing management of a complete network protection system that addresses the full range of threats to their computing systems’ security and integrity. As a result, most educational institutions are under-protected and exposed to significant risks.

**Lack Of Real Time Protection**

Conventional solutions typically utilize “host-based antivirus” (HAV) technology, which is provided by a software application that is loaded onto a user’s desktop computer or a server. HAV technology is useful for protecting systems against threats introduced by physical contact with a computer – such as via floppy, CD drives, or USB ports - but is not as effective in dealing with attacks that enter via the network. For example, most HAV software scans email messages as they arrive, but does not scan Web traffic, because the decrease in Web page download speed would be too severe. The same is true for HAV software deployed on “gateway” servers at the network edge, in conjunction with the firewall – they too scan email traffic, but do not scan Web traffic. As the percentage of virus attacks from Web traffic increases – estimated at 20% or more and growing – the importance of scanning all traffic, including Web as well as email, becomes paramount. Without the ability to scan real-time traffic for content-based attacks, educational organizations place themselves at great risk, despite their investments in host-based antivirus software.
High Price and Total Cost of Ownership

Cobbling together best of breed point solutions into an ad hoc security system is a costly endeavor. A complete system that includes firewall, VPN, antivirus, intrusion detection, content filtering, and traffic shaping can cost $20,000 for a relatively modest network, and well over $100,000 for large networks. On top of this are maintenance fees and subscriptions for antivirus, intrusion detection and content filtering updates. In addition, annual costs for skilled networking and security personnel can equal or exceed the initial capital expenses – presuming one can attract and retain these highly sought-after people.

Difficult To Implement And Manage

Diverse and complex systems made by different manufacturers will by their very nature tend to be difficult to manage. Policies of one application won’t manage those of another. Some systems (antivirus, content filtering, IDS) will need to be updated regularly while others will not. Different personnel will need to handle questions and problems with their systems – no one or two individuals are likely to understand the entirety of the solution. Finally, management of numerous remote deployments can make things even more challenging.

Note that a cottage industry has arisen around trying to solve this very issue, validating how difficult the challenge really is. Many startups are working feverishly to develop one, comprehensive management tool that will allow administrators to control the entire solution from (ideally) one interface. As yet, no one appears to have succeeded but the search continues.

THE FortiGate™ ANTIVIRUS FIREWALL ADVANTAGE

Fortinet offers a new approach to providing educational network protection at network speeds with award-winning FortiGate Antivirus Firewalls. Based on a revolutionary new architecture, FortiGate Antivirus Firewalls are ASIC-based network protection platforms that combine all of the capabilities necessary for complete, real-time protection at the network edge, including -

- Network Antivirus (NAV) Protection
- Firewall
- VPN
- Network Intrusion Detection
- Content Filtering
- Traffic Shaping

-delivered in integrated, cost effective, easy to install and maintain units with superior price/performance.

Fortinet’s Antivirus Firewalls sit on the edge of the network and scan all traffic entering and leaving the network in real time without degrading network performance. Instead of a patchwork system of point solutions with the inevitable holes and seams, Antivirus Firewalls are completely integrated units that act as the gatekeepers of the network’s
safety. They also bar inappropriate content from entering the network at all by scanning this content in real time as it tries to make its way to a user’s desktop. They provide ICSA-certified firewall and VPN functions and are the world’s first ICSA-certified antivirus gateways, providing the ability to scan both email and Web traffic in real time.

*Figure 1.4 Using Fortinet Antivirus Firewalls to stop viruses, worms and other malicious content at the network edge*

The network-based antivirus approach (“NAV”) utilized by Fortinet’s Antivirus Firewalls resolves the shortcomings faced by the HAV approach. FortiGate systems scan web and email traffic at the edge of the network in real time and before the traffic reaches any individual server or desktop. This allows the Antivirus Firewall to catch viruses and worms before they enter the network. In addition, because the Antivirus Firewall sits on the edge of the network, it can be updated automatically and as often as necessary in response to new threats. And because it is the “gatekeeper” of the network’s safety, it is the only platform that must be updated with a new virus signature thereby leading to a much shorter “window of vulnerability” (see figure 1.5 below).
Fortinet’s Antivirus Firewalls provide a complete solution that addresses the full range of threats to organizational institutions. Specifically, a single FortiGate Antivirus Firewall, easily installed and maintained at the edge of a campus network can be used to:

- Stop viruses and worms before they enter – or exit – the campus network
- Provide VPN services and scan tunnels for harmful content
- Block the use of campus networks for illegal file swapping and/or limit the amount of network bandwidth allocated to swapping applications
- Filter Web traffic for inappropriate content based on URLs, keywords, or both
- Alert administrators to attempts to compromise critical computing systems
- Support compliance with government regulations and qualify for special funding
- Limit exposure to liability caused by allowing inappropriate or malicious content to enter or exit the campus network

Fortinet’s Threat Management Team (TMT) operates around the world, 24x7 to identify new attacks and develop detection “signatures” that enable FortiGate units to stay current with new threats. Because FortiGate Antivirus Firewalls sit at the edge of the network, Fortinet’s FortiResponse Distribution Network (FDN) can “Push” updates at any time to all FortiGate units within minutes providing rapid, industry-leading response to fast-breaking attacks.
Fortigate Antivirus Firewalls are available to meet a wide range of needs, from entry-level models that are cost effective for the smallest schools, to multiport, multi-gigabit models that support high-availability and advanced networking features consistent with the needs of the most demanding, mission critical networks. Across the board, the price/performance provided by FortiGate Antivirus Firewalls makes it possible for educational institutions of all sizes to enjoy the highest level of network protection without compromising security, performance, or budgetary constraints.

FOR MORE INFORMATION

Business Information
Please visit us at www.fortinet.com.

Support Information
Please contact us at support@fortinet.com.

Potential Partners
Please contact us at partners@fortinet.com or visit us at www.fortinet.com.

Additional Resources
Please contact us at (1) 408.235.7700 for engineering/technical support.