Real Time Network Protection for Educational Institutions

White Paper

High Performance Multi-Threat Security Solutions

FORTINET

Introduction

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 while also not causing delays in time-sensitive traffic.

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. In contrast, Fortinet's FortiGate Multi-threat Security systems address all the network security needs by offering educational institutions the security and performance their environments demand. Fortinet's ASIC-accelerated FortiGate systems scan File Transfer Protocol (FTP), email, Instant Messaging (IM) and Web content at the network edge and in real time— protecting the educational network from threats and other inappropriate peer to peer or file sharing content before it can enter the network. Fortinet's Multi-threat Security systems combine firewall, VPN, Intrusion Prevention System (IPS), antivirus, Web filtering and antispam functionality in one easy to install, maintain and update platform.

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
- Introduction of viruses and worms into campus networks
- Utilization of campus networks for illegal content sharing
- Requirements to archive electronic communications for electronic discovery purposes

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 distributed and diverse educational network and computing 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 PC control.

Today, the most damaging and costly attacks do not require sustained connections from outside to inside the private network. "Content-based" threats, such as viruses, worms, Trojans and other malware deploy agents, often called "bots", 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 compared to instant Web downloads or instant messaging. For example, of the top 5 online activities in 2005 were "real time" activities - instant messaging, Web surfing or browsing, reading news, and accessing entertainment or social information.

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 through higher and adult education. These include protection from malware, secure connectivity between remote locations and the network, protection from inappropriate content and compliance with regulatory requirements, maximization of bandwidth and other network resources, protection of administrative resources and students from intrusions, ease of maintenance and updating, maximization of performance, and capital and expense budgets. Each of these challenges are analyzed separately below.

Protection from Malware

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. To make matters worse, attacks are increasingly "blended attacks", morphing the worst characteristics of viruses, worms, and network intrusions in powerful, multifaceted agents. Blended threats, examples of which include Nimda, Code Red and Slammer, 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 can easily 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, with conventional solutions 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. University IT administrators are struggling to keep up with this problem. According to a recent news article, an IT administrator at the University of North Texas claimed that technicians at the school were removing viruses from an average of 16 student computers every 90 minutes.

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. And it isn't getting any better in the near-term. While hard to pinpoint, estimates for the cost of virus damage has been increasing rapidly over the

last few years. Analysts and statistics companies estimated that the global cost caused by viruses and other malicious attacks in 2005 was as high as $52B and just one short year later, estimated the cost of eCrime to be as high as $60B.

In 2004, the MyDoom and Sasser viruses demonstrated the speed and reach of the newer types of attacks. Multi-faceted and extremely virulent, MyDoom was shown to infect 1 out every 12 messages in a test sample. It was quickly recognized by leading industry experts as having the worst impact of any virus outbreak since the Internet's inception.

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 peer-to-peer 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 or peer-to-peer protocols. Alternatively, traffic management technology can be used to limit the amount of bandwidth that is allocated to these types of applications.

Protection from Intrusions
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 Prevention System (IPS) can help identify hackers and stop them in their tracks. IPS 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 and allows the network administrator to take immediate action to protect the network. An effective IPS system will set off an alarm when network activity fits a known "attack profile" either automatically as part of a security policy or manually. Just as importantly, a truly effective IPS system can be configured to block threats from entering the network in either an automated or manual fashion.

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, security policies and capabilities results in a daunting and expensive management task that can require extensive staffing.

Regulatory Concerns
Another concern is the need for archiving of all electronic communications. In September 2005, updates to the Federal Rules of Civil Procedure (FRCP) require that electronic documents -- including e-mail and perhaps even instant messaging logs -- be available as evidence in civil court cases. Public schools are being asked to stretch their already thin budgets to now provide storage and retrieval capabilities of all transmitted messages for at least three years. Schools that do complete such projects will improve their ability to defend themselves if lawsuits are filed against them by students, their families or employees, by providing proof of electronic actions in the discovery process.

Challenges and Issues Specific to Higher Education

By contrast 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" or peer-to-peer protocols (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 used as 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. While the legal issues are somewhat in the "gray" area, recent developments would suggest the issue may be heating up. In early 2003, the Recording Industry Association of America (RIAA) began its piracy counter measures against educational institutions in 2003 when it sent letters to more than 2300 college presidents requesting that the schools "inform students of their moral and legal responsibilities to respect the rights of copyright owners."

The RIAA has followed up this initial salvo with even more aggressive efforts in its continued fight against file swapping and has started suing individual students in April 2005 for using the high-speed capabilities of Internet2 to share DVD movies. The International Federation of the Phonographic Industries (IFPI) has launched similar lawsuits in Europe and Asia and Japan has also begun legal action against people using peer-to-peer applications to trade copyrighted music and movies.

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 just a few years ago 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 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:

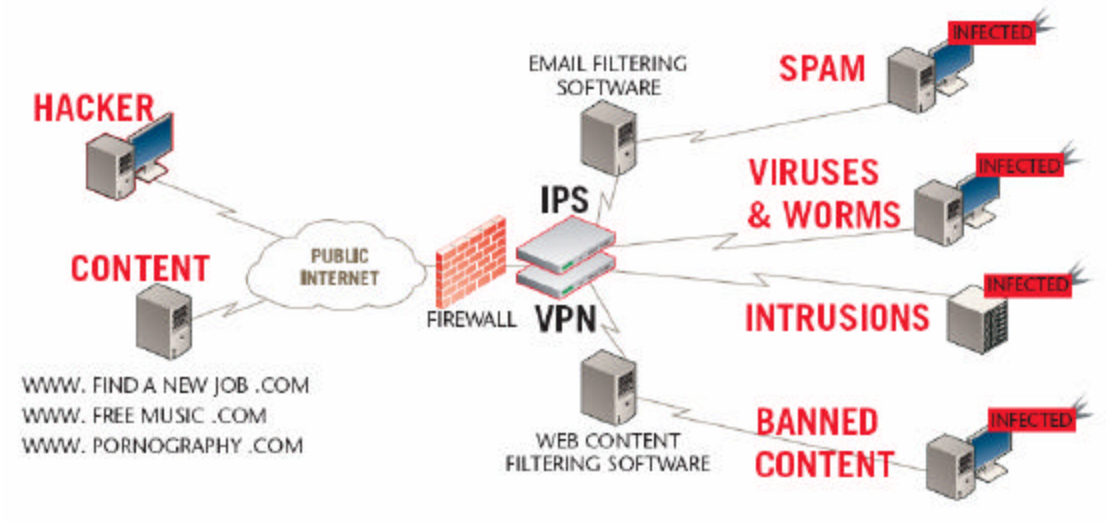

Figure 1: Point solutions cobbled together

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 annual 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/IPS) 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™ Multi-threat Security System Advantage

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

- Network Antivirus Protection (ICSA Labs Certified)
- Firewall (ICSA Labs Certified)
- IPSec VPN (ICSA Labs Certified)
- SSL VPN (ICSA Labs Certified)
- Network Intrusion Prevention System (ICSA Labs Certified)
- URL and Content Filtering
- Antispam
- Traffic Shaping

All capabilities are delivered in integrated, cost effective, easy to install and maintain units providing clearly superior price/performance. FortiGate systems sit at 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, FortiGate Multi-threat Security systems are completely integrated units that act as the gatekeepers of the network's security. 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 Labs certified firewall and VPN functions and are the antivirus gateways with the most ICSA Labs certifications providing the ability to scan both email and Web traffic in real time.

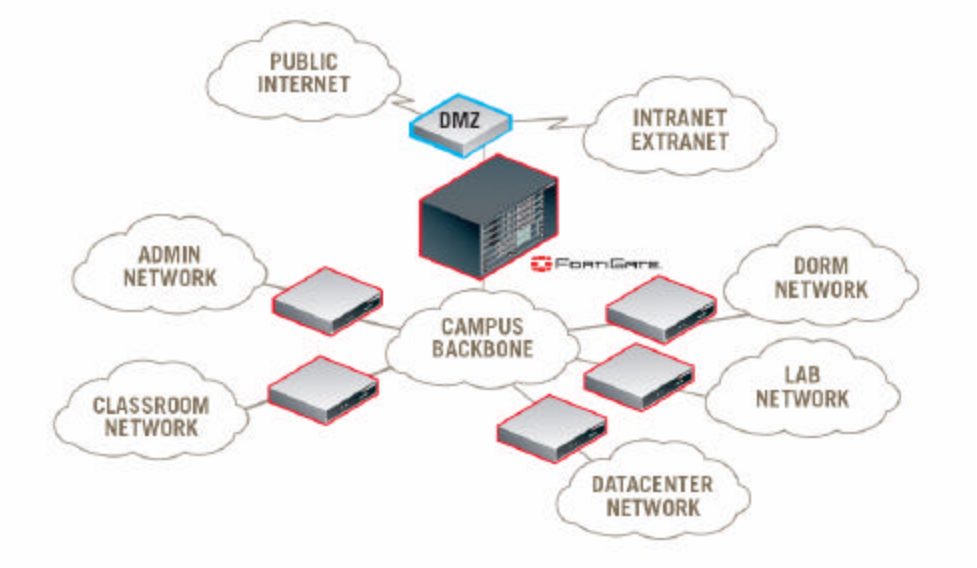

Figure 2: Using FortiGate Multi-threat Security systems to stop viruses, worms and other malicious or inappropriate content at the network edge and within the network. How a sample university can deploy a number of FortiGate units throughout its network:

1. A Fortinet FortiGate-5000 system at the gateway scans web, email and VPN traffic in real time for viruses, worms, inappropriate content, and intrusions. Alternatively, the unit could operate in "transparent mode" behind a legacy firewall system providing gateway antivirus protection (shown above); other functionality (VPN, firewall, intrusion detection and prevention, content filtering) can be "turned on" as necessary.

2. To prevent the spread of viruses into the administrative services, a FortiGate-800 system is installed behind the existing software-based firewall.

3. To provide an extra layer of protection within the network, a FortiGate-500A system provides firewall, antivirus and Intrusion Detection/Prevention at the Dormitory network gateway.

4. To protect mission critical data, a FortiGate-3600A system (or FortiGate-5000 system for large networks) provides firewall, antivirus and Intrusion Detection/Prevention security at the Data Center gateway.

Fortinet's integration of application-layer and network layer functionality revolves the shortcomings faced by the point "solution" approach. FortiGate systems scan web, VPN 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 FortiGate to catch viruses and worms before they enter the network. In addition, because the FortiGate 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, worm or intrusion signature thereby leading to a much shorter "window of vulnerability."

How Fortinet's Multi-threat Security systems Address the Needs of Educational Institutions

Fortinet's Multi-threat Security systems provide a complete solution that addresses the full range of threats to organizational institutions. Specifically, a single FortiGate system, easily installed and maintained at the edge of a campus network can be used to:

- Stop viruses, worms, Trojans, spyware and inappropriate content before it enters or exits the campus network
- Provide VPN services and scan tunnels for harmful or inappropriate 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 thereby qualify for special funding
- Limit exposure to liability caused by allowing inappropriate or malicious content to enter or exit the campus network
- Provide content archiving features to store messages and content embedded within emails, Web downloads, and Instant Messenger text and file attachments in an external storage device such as the FortiAnalyzer series of products

With Fortinet's FortiGuard™ Antivirus Service and Intrusion Prevention Service enabled, all antivirus signatures, IPS, and attack detection engines are kept up-to-date automatically. FortiGuard subscription services' automated updates eliminate the need to manually search for and update security content, greatly increasing the effective protection of the FortiGate system.

Because FortiGate Multi-threat Security systems sit at the edge of the network, Fortinet's FortiGuard Network can "Push" updates at any time to all FortiGate units within minutes; providing rapid, industry-leading response to fast-breaking attacks.

Additionally, FortiManager and FortiAnalyzer centralized management systems are available to provide central configuration management, as well as centralized logging, reporting and archiving of events and messages including message content such as: email text, Web URLs, Instant messenger text and downloaded file attachments.

FortiGate Multi-threat Security systems are available to meet a wide range of needs, from entry-level models that are cost effective for the smallest schools, to multi-port, 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 Multi-threat Security systems makes it possible for educational institutions of all sizes to enjoy the highest level of network protection without compromising security, performance, or budgetary constraints.

Education Customers Currently Using Fortinet's Multi-threat Security systems

Within a few months of introduction, Fortinet's Multi-threat Security systems earned rave reviews from educational customers all over the world a testament to their cutting edge technology, ease of installation and maintenance and overall value compared with competing solutions. Numerous major universities, school districts and schools are already securing their networks against viruses, worms, intrusions and inappropriate content utilizing Fortinet technology with many more in the process of doing the same. A small snapshot of Fortinet's extensive education customer base includes the following institutions:

- University of Ballarat (Australia)
- University of Hawaii (US)
- Soongsil University (Korea)
- Tam Kang University (Taiwan)
- Brigham Young University (US)
- Parma University (Italy)
- Fu Jen Catholic University (Taiwan)
- Florida Computer College (US)
- Widener University (US)

As shown by the glowing praise of the FortiGate line of Multi-threat Security systems, Fortinet's education customers are enjoying network protection that had not been possible before now:

"Before deploying the FortiGate systems, the Soongsil computer center's network faced at least one stretch of downtime a day due to traffic surges related to network attacks. In selecting a security gateway, we noticed that the FortiGate systems were the only hardware-based antivirus firewall systems available, which made them effective for handling Web traffic and other latency sensitive applications without impacting the performance of our applications. With the FortiGate systems deployed we have effectively blocked attacks from getting into our center and as a result our service levels have greatly improved."
- Lee Chang-don, IT Manager, Songsil University

"With the volume of email traffic generated by our schools, we quickly realized our current IT security system was not as flexible as required, so we looked to upgrade and chose Fortinet."
- Michael O'Connor, Network Manager, Medway Council

"Only a comprehensive solution providing antivirus, firewall, VPN and network intrusion detection can deliver the results we need for a student base expected to double in the next year. We evaluated several other products and found that the Fortinet systems provided the most complete, integrated, cost-effective security systems available. We were also greatly impressed with how easy the systems were to install - we needed only a few hours out of the days we had reserved for an upgrade involving this number of security applications. Fortinet has really cracked the code on making it easy and affordable to implement comprehensive network protection."
- Joseph Vega, Director of IT, Florida Computer College

"In servicing our communities as an ISP, as well as securing our own carrier-class network, Widener University needed effective enterprise security solutions capable of the most demanding uses. With Fortinet's FortiGate systems and FortiGuard Web filtering service, the comprehensive level of protection, combined with sheer robustness of product and high availability capabilities allows our university community to benefit from enterprise network protection tools with fewer concerns regarding down-time."
- Perry Drayfahl, Director of Technical Resources, Widener University

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated multi-threat security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, Web content filtering, VPN, spyware prevention and antispam—providing customers a way to protect multiple threats as well as blended threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified eight times over by ICSA Labs (firewall, antivirus, IPSec, SSL, IPS, client antivirus detection, antivirus cleaning and antispyware). Fortinet is privately held and based in Sunnyvale, California.

FORTINET
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700
Fax +1-408-235-7737
www.fortinet.com

WPR106-0707-R2