

Keeping the network secure and virus-free by deploying an in-front-of-the-router security edge platform



Security Market Key Issues

- **92,000 viruses and worm variants** (*McAfee Avert labs 2004) Market share is driving hacker decisions and large networking companies are the targets.
- **352+ router vulnerabilities exist today** (*CERT 2004) Large networking vendors are losing customer confidence because router exploit kits and stolen source code are publicly available. Routers have to broadcast their position and therefore will remain vulnerable.
- **94 percent of CIOs say their networks are at risk** (*Information Week study of 7,000 CIOs 07/2004) Network vulnerabilities are wide spread and change daily, increasing attacks deep within networks.
- **90 percent increased resource cost with multi-point solutions** (*Independent study by Tolly Group 07/2004) Fragmentation is increasing cost, security breaches, and the mean time to mitigate zero-day attacks.
- **83 percent of Internet traffic is malicious or unwanted e-mail** (*Internet Engineering Task Force (IETF) & Microsoft 09/16/2004 - Reuters News) IT departments are faced with moving targets that come in the form of denial of service (DoS), virus/worms, intellectual/asset loss, changing legislation and compliance regulations.
- **28 billion port scans happen every day** (*CERT 2004 study) Yet, applications continue to be deployed to the edge of networks exposing them to security breaches.
- **30 percent of all HTTP traffic is untrusted** (*Radware 2004) It uses critical and expensive bandwidth once it enters the network.
- **Organizations continue to size networks to handle unwanted traffic**

Hamline University

Hamline University has proven to be an innovative university with high quality, rigorous academics for the past 150 years. The University has more than 4,000 students, 300 faculty, and 250 administrative staff using a complex network environment with more than 11,000 e-mail accounts and 150,000 e-mails entering and exiting the network daily.

When students return to Hamline University after the summer break, they bring with them clothes, mementos of home, a computer or two and the ever-increasing possibility of computer viruses and worms. According to Anthony Schroeder, director of network services for the university, although the university has security policies in place, it would be impossible for IT staff to police individual computers to ensure they are being patched regularly and running a current version of an anti-virus program

The St. Paul-based university's ongoing need for enhanced network security was underscored by its access to Intertech, the State of Minnesota's Internet Service Provider for many colleges, universities, and government agencies within the state, including the Minnesota State Colleges and Universities (MNSCU). Through Intertech, Hamline University also has access to Internet2, a broadband second generation of the Internet.

"How do we make sure the information coming over is legitimate?" said Schroeder. "Just think what a virus could do if it had a pipe right to your front door."

Compare and Contrast

With these concerns uppermost in his mind, Schroeder began requesting information from firewall vendors over the summer of 2004. As brochures piled up on his desk, Schroeder started investigating the DeepNines Security Edge Platform™, which promised the capabilities of a behavioral-based firewall coupled with anti-virus protection and a pro-active approach to security in front of the router. The platform also features management and tracking tools.

"DeepNines Security Edge Platform is all about being able to keep everything flowing nicely," said Schroeder. "They focus on known and unknown vulnerabilities in front of the router."

As a technologist, Schroeder was interested in the technology behind the DeepNines Security Edge Platform and thought the solution would be something the university could purchase as part of its future security plans. However, having determined the breadth of the solution's capabilities and its competitive price, Hamline University decided to buy DeepNines' platform instead of a separate firewall. Schroeder noted that it offered an array of integrated security functionality in one platform versus having to work with a separate firewall, intrusion prevention/detection or commodity anti-virus provider. DeepNines' solution was more cost beneficial than that approach, and it fit within the university's budget.

Industry:

Higher Education

Number of Users:

4,000 students, 300 faculty and 250 administrators

Security Problem: Lack of Intrusion Prevention and Firewall

Students could not be relied upon to regularly patch their computers or run current versions of anti-virus software. This threatened the security of the university's network and MNSCU, its access to Internet2.

Solution:

The DeepNines Security Edge Platform™

Business Benefits Gained:

Dramatic savings in overall total cost of ownership and lower administrative time

- 50 percent reduction in overall capital expense
- 80 percent reduction in annual operational expense
- 160 percent reduction in annual maintenance administration expense
- 100 man-hours saved in support and administration per month
- Collaborative relationship with DeepNines Technologies
- Increased application service reliability and availability
- Slashed the risk of viruses and worms
- Enabled the university to better track network traffic and understand bandwidth patterns
- Maintains network performance and integrity even under attack

HAMLINE UNIVERSITY

DeepNines Solutions

DeepNines is the market leader in perimeter security and the first and only technology company to deploy a comprehensive security platform in front of the router. DeepNines Security Edge Platform™ integrates intelligent firewall, intrusion prevention, best-of-breed secure content management, forensics and reporting. It operates outside the network infrastructure, improving an organization's security "deep into the nines."

The Security Edge Platform, a patent pending security system, is a fully automated intrusion prevention and traffic management system and serves as a single, centralized security and traffic management system for an entire organization.

DeepNines Security Edge Platform Key Features:

- Logically located in front of the router, allowing good traffic in and keeping bad traffic out
- Zero Footprint Technology™ (ZFT) does not require an IP or MAC address, making it invisible and impervious to attacks, yet easy to administer and install
- Protects and blocks against known and unknown vulnerabilities or zero-day attacks
- Deep packet inspection evaluates each packet entering and exiting the network
- Secure Content Management includes best-of-breed anti-virus, anti-spam, and content filtering
- ForensiX Capture System™ (FCS) captures all network traffic for regulatory, legislative and forensic reporting requirements
- Holistic Management Console™ (HMC) provides integrated management and monitoring components of bandwidth, security condition, and signature updates or upgrades with granular control and graphical views

Financial Value Provided by DeepNines Technologies:

- Reduce capital expenses by 50 percent
- Reduce annual operational cost by 80 percent
- Reduce annual administration expense by 160 percent (Tolly Group)
- Reduce requirements on network infrastructure
- Reduction in losses and cost avoidance associated with malicious traffic
- Reduce total cost of ownership

Nuts and Bolts

Hamline University uses Cisco Catalyst 3550 switches to connect, via gigabit fiber, to a Cisco Catalyst 4500 switch managed by Intertech at the University of Minnesota. Hamline's far-reaching network also includes a 3Com 10/100 switch, Broadcomm ports and several 100Mb VLANs. The University of Minnesota connection gives Hamline University access to other MNSCU colleges and universities, as well as Internet2.

"DeepNines' Security Edge Platform sits on a gigabit copper VLAN in front of our software base firewall," according to Schroeder. "By positioning the DeepNines platform here, the university proactively prevents infection and performance degradation, something that no other solution in the market can provide to protect router vulnerabilities. They are so intent on partnering with educational institutions they gave us the option to fly in a technician to help through the evaluation process so that we got the full breadth of knowledge and capabilities about the system."

The university also worked with Roseville, Minnesota-based Collier Computing, a Sun Microsystems Inc. iForce and DeepNines Solution Provider partner that it had teamed up with on previous Sun purchases and installations.

"DeepNines allows you to test drive the solution, and gives you some smarts to show you what you're doing. Most other security vendors send you the equipment and it's left to the customer to deploy it without hands-on guidance from the manufacturer" he said. "What we were looking for was a firewall to help protect us from outside threats and also another product to let us know what was happening on our network. DeepNines' solution had both functionalities. They also offer an additional piece which is anti-virus scanning for e-mail."

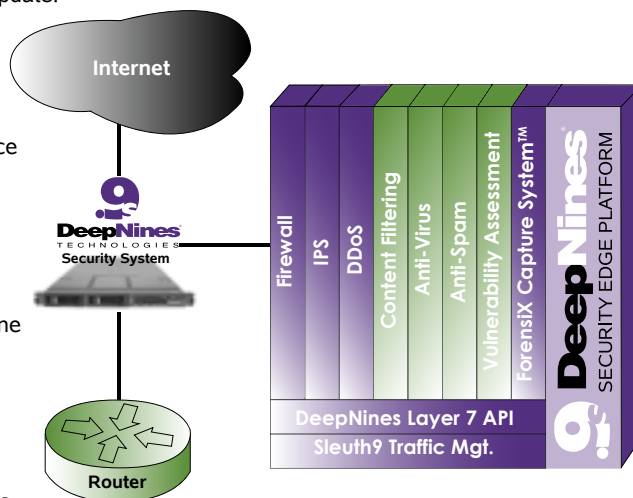
Putting It in Place

"Despite its sophisticated features, installing the DeepNines Security Edge Platform was simple. A DeepNines technician did the actual implementation for the university," said Schroeder. "This left the two-person network department which is responsible for the network, Internet connections and many of the university's servers free to do other tasks. Their Zero Footprint Technology™ (ZFT) allows for easy plug-and-play due to the fact that we did not have to make any changes to the network," he said. "Additionally, their integrated anti-virus engine thrived on, we did not have to change the mail-servers IP addresses or wait for any DNS update."

"DeepNines has been on the ball since day one," Schroeder said. "Their tech support is top notch."

Hamline University expects to reduce the time it spends maintaining its network security, said Schroeder. The management and tracking reports will help the university monitor its network traffic without forcing the network staff to spend hours watching a screen to determine traffic patterns, he noted.

"Because there are only two of us taking care of the Internet network and most servers, we rely on the technology to do some of the work for us," said Schroeder. "DeepNines Technologies pricing model will immediately save us 50 percent on capital expense and approximately 80 percent on annual operational expense. As for our time, it's priceless."



Conclusion

Hamline University, which was named the top-ranked Minnesota University in its class by U.S. News and World Report magazine for the fourth consecutive year, is now assured it has taken the necessary steps to prevent its students from inadvertently infecting the internal network or Internet2. The university's ongoing partnership with DeepNines Technologies allows its small network department to use its time more productively, rather than on maintenance, security management issues and putting out fires, said Schroeder.

"Now that we have the bandwidth available, it's just a question of imagining what to do with it," said Schroeder. "Thanks to DeepNines, I can spend less time focusing on day-to-day security issues and more time looking into the possibilities Internet2 offers us."



www.deepnines.com
14643 Dallas Parkway Suite 150, LB 76
Dallas, Texas 75254
1-866-DEEP912 or 214-273-6996