

Stanford University School of Education Stops Spam, Viruses and Network Intrusions at the Perimeter with Juniper Integrated Security Devices

**Organization:**

Stanford University School of Education

Industry:

Education

Challenge:

Reduce the torrent of spam, viruses, phishing and network attacks unleashed while maintaining ready access to the Stanford University School of Education network

Solution:

Juniper Networks Secure Services Gateway 550 integrated security device

Benefits:

- Stop spam, viruses, phishing and network attacks at the perimeter, preventing them from entering the network
- Ease the administrative burden of making sure 550 to 700 users have updated anti-virus and anti-spyware software on their desktops and laptops
- Maintain open access required for academic collaboration

As an internationally distinguished institution, the Stanford University School of Education is a prime target of wannabe hackers and proficient attackers who bombard the university e-mail systems with viruses, spam, phishing attacks, worms, and other malware, hoping to steal intellectual property or to simply make a name.

Yet as a research institution, the School of Education must allow its faculty, students, and visiting professors to collaborate easily with each other and across departments, and have ready access to information systems across the university. Students and faculty use a wide variety of applications on their desktop and mobile computers, ranging from officially sanctioned applications like e-mail and courseware to personal applications like VoIP and peer-to-peer software.

The IT team at the School of Education must strike a delicate balance between protecting users while giving them the freedom to use the computing tools they need. That balance makes it all the more difficult for IT to protect the School of Education against the rising tide of malware and network attacks.

At the Stanford School of Education – like many organizations whether academic or corporate -- some 80 percent of incoming mail is spam and other unsolicited e-mail. “Spam is totally out of control,” says Dr. Paul Kim, CIO for the Stanford University School of Education. “The spam coming in nowadays is more sophisticated and the spam filters on our e-mail servers aren’t catching it.”

If the spam filters are set too loosely on the e-mail servers, then users receive an avalanche of unwanted mail and they waste time deleting it or creating spam folders. If the spam filters are set too tightly, then users run the risk of losing important e-mails. "Spam wastes a lot of time and causes user frustration," observes Kim.

Spam causes more than wasted effort. Spam can be inappropriate, offensive – and dangerous. These unsolicited e-mails carry payloads of malware – worms, Trojans, viruses, and spyware. They can be phishing attacks designed to trick an individual into giving up personal information, which criminals will use for identity theft and fraud.

In several instances, worms have penetrated the university's defenses and compromised vital systems. "As a research institution, we have to protect our intellectual property," says Tony Wong, network administrator at the School of Education. "Spam, worms, malware, and network intrusions are on the increase, so we have to take action."

The Solution

Stanford turned to Juniper Networks Secure Services Gateway 550 (SSG 550) to provide an integrated perimeter-based defense that bolstered its desktop- and server-based protection against these damaging threats. As a longtime Juniper customer, Kim was eager to migrate the school's existing Juniper firewall/VPNs to the integrated networking and security of the SSG 550.

The Juniper SSG 550 is a purpose-built security appliance that delivers high performance, security, and LAN/WAN connectivity. Traffic flowing through the SSG 550 can be protected from worms, Spyware, Trojans, and malware by a complete set of Unified Threat Management (UTM) security features including Stateful firewall, IPSec VPN, IPS, Antivirus (including Anti-Spyware, Anti-Adware, and Anti-Phishing), Anti-Spam, and Web Filtering. The SSG 550 is designed for regional and branch office deployments.

"The SSG 550 is a one-stop solution," says Wong. "Integrated security devices just make sense. As a result, we're able to put the proper levels of security in place while allowing users access," says Kim.

The SSG 550 appliances are located in the School of Education's DMZ, where they eliminate spam, spyware, and other malware before they can get onto the network and compromise vital networks and systems. Protecting the internal network is critical because university's network is a single, flat network. To facilitate academic collaboration, the university does not use VLANs to isolate different departments' traffic.

The Juniper SSG 550 appliances provide a strong layer of protection to the university's current server and desktop anti-spam and anti-virus protection. Departmental servers and users' desktops and laptops have individual firewalls and anti-virus software. Desktops and laptops also have anti-spyware protection.

The Benefits

Before rolling out the SSG 550, the e-mail servers themselves were also responsible for filtering out the spam, and were under increasing load because of spam. Now that the mail servers are offloaded from their spam duty, the School of Education has been able to extend the life of its e-mail servers. Legitimate e-mails sail through, and the SSG 550 stops spammers and phishers at the gateway.

"The SSG 550 has delivered a significant hard-dollar saving that is multiplied across hundreds of users," says Wong. The reaction from the faculty and students has been overwhelmingly positive because they have experienced a reduction of junk in their mailboxes. Plus, network bandwidth and server resources are not wasted.

Because the SSG 550 has network and application level protection, IT can better contain attacks and gain visibility into hackers' activities. "We can monitor an attack and contain it," says Wong.

Before deploying the SSG 550 appliances at the gateway, IT had the unenviable task of making sure 550 to 700 users had up-to-date anti-virus and anti-spam software installed on their desktops and laptops. "It was a lot of work to monitor the users to make sure everyone was downloading the updates," says Wong.

Managing the SSG 550 appliances is straightforward. "We can see what's coming into our network and what's going out. To get that visibility without the SSG 550, we had to visit every desktop and server individually," says Wong. The IT staff uses either the SSG 550's Web-based interface or the command-line interface. The NetScreen-Security Manager can also be used to control all aspects of the SSG 550, including configuration and security policy.

Stanford can be confident in the high performance SSG 550 appliances as its needs grow. The SSG 520 delivers 600 Mbps of firewall traffic, 300 Mbps of IPSec VPN and 300 Mbps of deep inspection IPS. The SSG 550 delivers 1 Gbps of firewall traffic, 550 Mbps of IPSec VPN and 550 Mbps of deep inspection IPS.

"We think integrated security is a model for other educational institutions. The SSG 550 solution helps us maintain the open environment that the university needs to do research and teaching," says Kim. "Opening the network for academic purposes is a challenge for IT administrators because you put yourself at risk. In a corporate environment, you can close everything. We have to meet the diverse needs in the university."



CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100

www.juniper.net

EAST COAST OFFICE

Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501