

WE GET PRINTERS.  **HP LaserJet Pro P1102w \$148.99** **CDW-G PEOPLE WHO GET IT** [Shop Now](#)

Sign up for the
Higher Education
E-Newsletter [GO](#)

EDTECH™ FOCUS ON HIGHER EDUCATION

search...

[GO](#)

[EdTech](#) [CDW-G](#)

Monday, July 11, 2011

[HOME](#)

[MAGAZINE](#)

[RESOURCES](#)

[E-NEWSLETTER](#)

[TECH TIPS](#)

[21ST CENTURY CAMPUS](#)

[CASE STUDIES](#)

[SUBSCRIPTIONS](#)

[PRINT](#)

[EMAIL](#)

TECH TRENDS

[DIGG THIS](#)

[SAVE TO DELICIOUS](#)

[SEED NEWSVINE](#)

Control and Conquer

Next-generation firewalls provide fine-grained visibility into applications.

By Karen D. Schwartz

Until last year, Berry College's firewalls were just one item in a vast arsenal of security tools that included intrusion prevention devices, traffic shapers and traditional routers. When that arrangement became difficult to manage, the IT department upgraded its SonicWALL firewalls to the latest technology — new dual SonicWALL E-Class NSA E6500 units, which combine advanced firewall functions with intrusion prevention and other capabilities.

[June 2011 E-newsletter](#)

[Protecting Portables](#)

[Control and Conquer](#)

[Core Cisco ASA Commands](#)

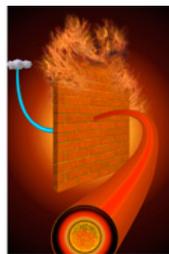
[SonicWALL NSA E5500](#)

"Instead of having multiple devices, we rolled all of that into our firewalls and really simplified our architecture," says Dan Boyd, senior network architect for the college in Mount Berry, Ga. "Now, our metro Ethernet ISP connections come straight into the firewall, with no routers needed, and all of our traffic management is done from one box."

The idea of rolling intrusion detection, antivirus and protocol filtering along with firewall protection into a single device is one of the factors that has prompted organizations of all types to deploy next-generation firewalls, says Jeff Wilson, a principal analyst at Infonetics Research. Unlike earlier models, next-generation firewalls also provide a much more granular level of application inspection and control — down to the individual user. They also provide greater levels of manageability and flexibility.

Consolidating Boxes

Application control was another reason for Berry College's firewall upgrade. Not only can the IT department better identify and keep out applications that aren't tolerated due to policy, such as BitTorrent traffic, but it can give priority to important applications, such as the student data system and the college's customer relationship management system.



"With the latest revision of firmware to our device, we have very fine-grained control and great visibility into the network," Boyd says. "For example, if there is a spike in YouTube traffic, we can determine whether that's coming from a classroom as part of a class, or from a residence hall."

When Sam Houston State University first installed its Juniper Networks SRX 5800 firewalls in 2009, application control wasn't even on Information Security Officer Tim McGuffin's radar. He quickly realized the benefits, however, when use of peer-to-peer applications and video conferencing began growing quickly. It was then that he truly appreciated the ability to monitor applications and dynamically control traffic.

McGuffin's team originally bought the Juniper firewalls to address staggeringly high network growth (the school's network traffic routinely doubles every 12 to 18 months) and to improve performance and manageability.

"We started with a homegrown Linux iptables box and

8,000-plus

then got some basic firewalls, but intrusion protection was a limiting factor, and we outgrew them quickly,” he says. “They just couldn’t keep up. Every time we reached capacity we had to do a complete rip-and-replace, and it just didn’t make sense anymore.”

The number of security vulnerabilities documented in 2010, a 27 percent increase over 2009

SOURCE: IBM X-Force 2010 Trend and Risk Report (March 2011)

Because of fast network growth and a diverse client base, McGuffin sought firewalls that could provide high availability. “We needed to support multiple network types through the same device, since we support not only our administrative network and a research network, but we serve as an ISP for our residence halls and wireless clients. We really needed something with [10 Gigabit Ethernet] ports, which the firewalls had.”

And like Berry’s Boyd, McGuffin also was looking to consolidate security products. “We wanted an all-in-one box where you could enable and disable the features you wanted, depending on the circumstances,” he explains. “With this pair of firewalls, we can disable or enable IPS functionality if we need high bandwidth and low latency between two zones, or we can enable deep packet inspection when we need it.”

Smart Selection

Most organizations already have at least one firewall in place, but new pressures and requirements often make next-generation models attractive. When considering what to buy, keep these points in mind:

- Make sure the product has, at a minimum, a zero downtime configuration; support for user-based policy controls; the ability to identify applications and enforce network security policy at the application layer; full intrusion prevention; and good scalability.
- Determine the type of applications you need to control and how granular you need that control to be.
- Consider replacing your intrusion prevention system with the functionality integrated into a new firewall. This reduces complexity and makes management easier.