PRINT EMAIL

88 DIGG THIS
SAVE TO DEL.ICIO.US
SEED NEWSVINE

TECH TRENDS

Unified Threat Management

UTM devices save agencies money and simplify management.

By Karen D. Schwartz

For Roland Welsch, moving to a unified threat management system not only made sense for his security needs but also from a budgetary standpoint.

Welsch, IT manager for Jefferson County, Wis., was looking to replace a firewall and subscription to a web-filtering service. He decided on two Fortinet FortiGate 800 appliances, which offer not only firewall and web filtering, but antivirus, intrusion prevention and secure virtual private network connectivity.

"We were initially looking for a way to cut costs for our firewall, but found that not only were we able to replace our expensive web security product, but get everything else the UTM offered as well," Welsch says.

After implementation, Welsch calculated that he was saving more than $25,000 per year in support costs while adding functionality — a win-win proposition.

For cash-strapped state and local government agencies, which often have limited IT staff, UTM devices tend to be a great fit. These network security devices generally combine a firewall, VPN, intrusion detection and antivirus capability into one device. Manufacturers such as Check Point, Fortinet, Juniper Networks, McAfee, SonicWall and WatchGuard offer the hardware.

Because the products have multiple applications in one appliance, the organization simply plugs one box in at a remote site and then manages the device remotely. What's more, IT can buy just the features it needs without investing in multiple hardware devices. UTMs can be configured to handle the security applications organizations need, such as URL filtering and antispam, says Charles Kolodgy, research director for secure products at IDC. The appliances are modular, allowing organizations to use just what they need and add more later.

UTM products are expected to make up 33.6 percent of the total network security market by 2012, compared with 22 percent in 2008, according to IDC.

The business proposition for the city of Lincoln, Neb., was somewhat different. Although budgets are always tight, Lincoln's IT staffing is even tighter. That was the impetus for Jeff Jones, the city's network supervisor, to turn to SonicWall's NSA E6500.

"We have a small IT staff, and I'm the only one dedicated to networking," he says. "This is simple to manage, and that's important when I'm the only one managing it."

Jones said the most important features of the UTM for the city of Lincoln are preventing viruses and malicious attacks on the network. The system is fairly transparent, except for content filtering, which stops users from going to suspicious sites.

And more security benefits are forthcoming. Kolodgy says UTM devices are moving toward virtualization, which will allow users to easily turn security features on and off. The devices will also allow IT to use products from different manufacturers so they can pick the best of breed for each function.

Finding the Right UTM Fit
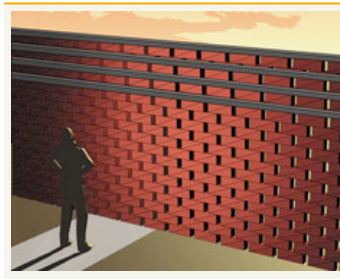
- Choose a tool that focuses on the capabilities that are most important to your organization.
- Pick a manufacturer whose technology road map matches yours.
- Test drive the management console and make sure it's a good fit for your organization.
- If you have strong preferences for specific security features from certain manufacturers, factor that into the mix.
- Consider the performance specifications of the appliance. The more applications you use, the greater the workload on the device.
- Evaluate the networking features in the box. Can you use the UTM to replace a router or wireless access point? If so, the solution will be more cost-effective.
- Look at the subscription process for the applications you need, not just the initial price of the box.