

the SENTINEL



POWERFUL NETWORK DESIGN, SECURITY AND ACCESS CONTROL SOLUTIONS

INTO THE BREACH

Unified threat management appliances help organizations plug security holes.

Remember the Little Dutch Boy who stuck his finger in the dike and saved the countryside from flooding? In many ways, he has become the role model for the evolution of network security. The traditional approach to defending systems has been to deploy a new dedicated security point product each time a security hole opens up.

The problem, of course, is that sooner or later you're going to run out of fingers.

Given the growing complexity of modern-day security threats capable of simultaneously exploiting multiple vulnerabilities, there aren't enough kids in all of the Netherlands to keep the flood of spam, malware and other threats from pouring in. That's why many organizations and solution providers today are

looking to stem the tide of network threats through a consolidated solution.

Integrated Approach

Unified threat management (UTM) devices are all-in-one systems that combine firewalls, anti-malware software, intrusion protection systems, content filters and more into one unit that can be easily managed through a single console. These devices offer integrated management, monitoring and logging capabilities, and streamlined deployment and maintenance that can be tailored to keep up with evolving security threats. Single-console management makes it easier for administrators to enforce detailed security policies throughout the organization, and eliminates the need to investigate multiple alerts generated by various systems from a single event.

"UTM devices allow organizations to enjoy end-to-end security without the cost and complexity of point solutions," said Jeffrey Reed, President, Classic Networking. "Solutions such as SonicWALL's NSA and E-Class NSA series of appliances give you everything you need to protect against malware, spam, Web-based exploits and other threats. Automatic security updates protect against emerging and evolving threats without administrator intervention."

With the integration of multiple

continued on page 2

CommunicationWorks

PRSR1 STD
U.S. POSTAGE
PAID
Tulsa, OK
Permit No. 2146

Into the Breach

continued from p. 1 ...

security engines into a single appliance, UTM also makes it possible to detect blended threats that employ a combination of attacks — such as a mix of viruses, worms, Trojans and denial-of-service attacks — crafted to circumvent a single line of defense. With UTM solutions, the integrated security engines work together, enabling the system to inspect real-time traffic from multiple vantage points. For example, a seemingly harmless e-mail that would pass through any anti-virus system could contain an HTML-based attachment that ultimately points to a Trojan. Because a UTM solution can use a combination of anti-spam, anti-virus, anti-spyware and other security engines, it can detect such blended threats more readily.

Closing the Gap

It has been largely unavoidable that most organizations wound up with a security infrastructure composed of numerous, disparate, disconnected countermeasures. Denial-of-service attacks and worms led to intrusion prevention and vulnerability management systems. Firewalls and anti-virus drove the need for virtual private networking. Soon came instant messaging, P2P file sharing, and a dramatic rise in spam. Now there is information leakage, phishing and spyware.

A patchwork approach to security is simply not sustainable, however. Operating, maintaining and coordinating multiple security products leads to runaway costs. And since point products are configured separately, conflicting or incomplete rule sets can result in significant network security gaps.

A UTM implementation can lower operating costs and standardize the security platform across even dispersed organizations. It can also achieve consolidation, reduce complexity, improve intrusion detection and provide load balancing integrated into a single system supporting multiple applications.

“SonicWALL has taken these capabilities to the next level,” said Reed. “Unlike single-processor designs that limit protection and degrade performance, SonicWALL’s Reassembly-Free Deep Packet Inspection technology utilizes a multi-core architecture to scan packets in real time without stalling traffic in memory. Load balancing classifies and

routes application-, file- and content-based traffic onto multiple security cores in real time, providing robust threat protection for bandwidth-intensive and latency-sensitive applications.”

Not Just for SMBs

Small to midsize businesses (SMBs) have been among the first to adopt UTM appliances due to their all-in-one functionality, easier management and attractive price points; enterprise organizations have been slower to adopt them. With more IT staff and larger budgets, enterprises are better positioned to absorb the costs of managing multiple best-of-breed security products.

Enterprise organizations have also had other reasons to snub the earliest versions of UTMs. For one, the first UTMs could be bandwidth hogs, reducing network performance by 10 percent or more when the full set of security services were in use. Another concern was the impact of packet inspection and reassembly on VoIP traffic.

However, the latest generation of UTM devices addresses those concerns. For example, SonicWALL’s E-Class appliances deliver reliable and scalable throughput for high-speed, widely distributed environments. These solutions also provide capacity for thousands of concurrent VPN connections and fully support voice over IP.

Although unified threat management can increase security, reduce costs and streamline management, it isn’t a panacea. IT security will never be a set-and-forget proposition. It requires constant vigilance, continual assessment and continuing education. But with today’s UTM appliances, organizations have another powerful tool for holding back the rising tide of security threats.

A patchwork approach to security is simply not sustainable. Operating, maintaining and coordinating multiple security products leads to runaway costs.

The Sentinel

Copyright © 2009 CMS Special Interest Publications. All rights reserved.

Editorial Correspondence:

4941 S. 78th E. Ave.,

Tulsa, OK 74145

Phone (800) 726-7667

Fax (918) 270-7134

Change of Address: Send updated address label information to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission. The Sentinel is published bimonthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

Enabling Remote Access

Increased mobility and regulatory compliance demands continue to drive SSL-VPN adoption.

You can't blame IT managers for wanting to lock down access to the network, given the endless barrage of increasingly sophisticated security threats they must attempt to thwart. At the same time, organizations are demanding anytime, anywhere access to mission-critical applications in order to maintain business productivity and ensure operational continuity.

These real-world requirements, combined with increased regulatory standards for remote access, are making Secure Socket Layer (SSL) virtual private network (VPN) solutions a business-critical component of the security infrastructure. SSL-VPN technology combines SSL — the encryption and authentication technology built into every Web browser — with access control, security policy enforcement and other tools to create secure connections to the corporate network via the public Internet. Although they are more limited than other remote access solutions, SSL-VPNs come with fewer headaches, making it feasible for organizations to provide remote access without increasing security risks or IT support woes.

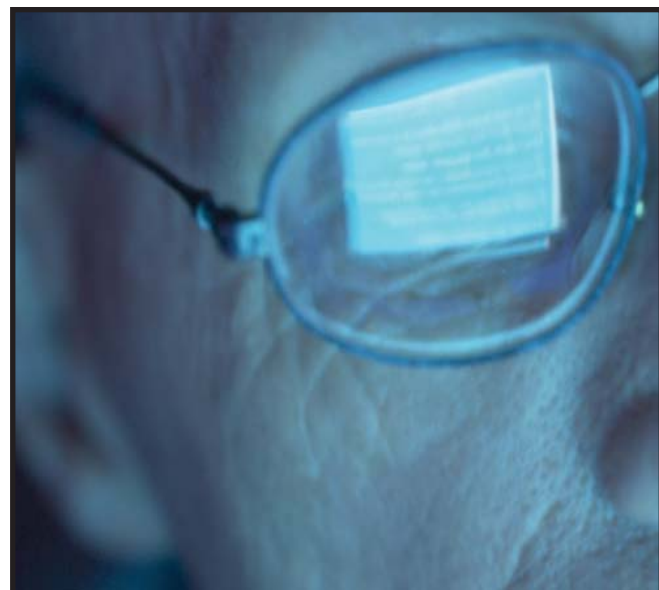
Traditionally, companies have provided secure remote access through VPNs based upon the IP Security (IPSec) suite of protocols. IPSec VPNs establish secure “tunnels” for private communications over the public Internet, providing end-users with highly secure access to network resources as if they were physically connected to the corporate LAN.

However, IPSec VPNs require that client software be installed on the end-user's machine — software that is notoriously difficult for the IT department to manage and the end-user to operate. In addition, IPSec VPNs often require special firewall configuration to allow public IP addresses to come through.

With SSL-VPNs, the remote user's interface is a standard Web browser. There's no learning curve because almost all users are familiar with browsers, and the IT department doesn't have to install and maintain any client software. What's more, the end-user can access the network from any Internet-connected device.

SSL-VPNs don't allow the deep network access enabled by IPSec VPNs — many products only support browser-friendly applications. However, most mobile users only need access to e-mail and a few other Web-based applications. SSL-VPNs allow IT departments to provide that level of access without the hassle of assigning and maintaining laptops.

SSL is not expected to eliminate IPsec anytime soon. Nevertheless, the SSL-VPN market will continue to see steady growth and acceptance as corporations are forced to deal with regulatory and security challenges in providing remote access.



HOW SECURE IS YOUR NETWORK?

Take advantage of our winter special on external assessments to learn exactly where the holes are in your network security and how to plug them.

We'll scan up to 24 IP addresses — normally a \$2995.00 service — **NOW ONLY \$1,995** if booked and scheduled by March 31!

Using network- and host-scanning tools, Classic Networking experts look for tens of thousands of possible vulnerabilities in operating systems, servers or firewalls to help ensure no one is accessing your sensitive information from a remote site.

Call us and take advantage of this remarkable value today!



(877) CNI-9250
www.classicnetworking.com



we protect your digital worlds

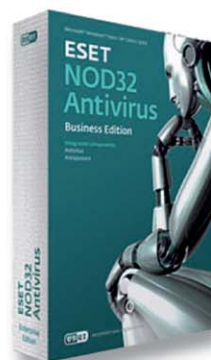
THE SMARTEST
IT MANAGERS DON'T
MAKE PROBLEMS GO AWAY.
THEY MAKE SURE
THEY NEVER APPEAR.

Today, 15,000 new internet threats will be created to attack your network. Predicting and intercepting these future threats is what we do. In fact, ESET® NOD32 Antivirus, with its industry-leading ThreatSense® technology, is the scalable security upgrade IT Managers are turning to for faster, more precise, and proactive protection against viral threats.

Contact your Classic Networking representative today to schedule a free trial!



(877) CNI-9250
www.classicnetworking.com



**ESET
NOD32
Antivirus
Business Edition**

A New Way To Think Smart



Proactive + Precise + Lightweight + Fast