



CMP

United Business Media

SECURE ENTERPRISE

BUILDING TRUSTED BUSINESS

WWW.SECUREENTERPRISEMAG.COM | MAY 2005

X TREME FIREWALLS

Unified threat-management devices promise to deliver three-pronged protection without bogging down your network. ISS's bargain-priced Proventia led a mostly mediocre pack

[BY MIKE FRATTO]

UTM perimeter-security devices combine firewalling, antivirus, and intrusion detection and prevention on a single appliance. Many throw in content filtering and antispam, making a compelling argument for one-stop security shopping. *Unified threat management*, a term coined by IDC, is not a new concept, however: Vendors have tried to bring these processes together for years but were stymied by performance problems. Fortunately, advances in processing, both on the main CPU and in specialized silicon, mean that performance problems can be overcome.

To see how well vendors are taking advantage of new technologies,

we tested UTM products in our Syracuse University Real-World Labs®, rating each on how well it increases protection without hurting performance. Unfortunately, we found most products wanting. Our scenario was typical: An organization with 5,000 users seeks an edge device that provides firewall, IDS/IPS, antivirus and content filtering. The organization’s DMZ network hosts DNS and Web servers that communicate with a back-end Microsoft SQL Server and an SMTP server, which relays mail to an internal Exchange 2000 server (for more details, see “Test Methodology,” page 4). Most traffic is from internal users to the Internet.

We invited 11 vendors to participate. Fortinet, Internet Security Systems, Secure Computing, SonicWall and Symantec accepted our invitation. Check Point Software Technologies, Cisco Systems and Finjan Software said they couldn’t ship products in time. Juniper Networks doesn’t have an offering that fits, and Astaro and iPolicy Networks did not respond to our invitation.

Advanced Protection?

It’s time to puncture the IPS myth: All the problems inherent in intrusion detection are exacerbated by automated prevention. Certainly, there are signatures that flag malicious traffic with a high degree of probability, and you can safely block these packets. Any protocol violation—for example, characters not defined within the HTTP protocol specification, similar to RFC 822—can be intercepted with little risk of a false positive.

Figuring out which other signatures can be safely blocked takes a bit more digging to determine if normal traffic will

trigger an alarm.

The vendors in this review take a conservative approach to setting default block policies, and that’s appropriate. Each network is different, and an aggressive cookie-cutter stance will likely turn away legitimate traffic. With the exception of ISS’s Proventia, changing the default action in the IPS functions of the devices tested was a simple matter of selecting the signature, or in some cases a family of signatures, and setting the ac-

Only Proventia properly detected our malicious traffic. The others failed to detect at least one attack. This is inexcusable.

tion to block. Changing the default IPS setting in Proventia is a multistep process, but it can be done.

However, in our tests only Proventia properly detected our malicious traffic. The other products failed to detect at least one attack—Fortinet’s FortiGate-800 came in last, detecting just two out of five. This is outcome inexcusable: All the vulnerabilities we selected are at least a year old, with publicly available exploit code waltzing through most of these devices and returning a reverse shell on our “attacker’s” computer. Moreover, we told all the vendors we’d be using publicly available exploits against servers with known vulnerabilities.

After testing, we shared our results, the tool we used (Metasploit 2.3) and the modules with the vendor participants. Frankly, if we didn’t provide the vendors with this information, we aren’t convinced they would have added new signatures. In

THE ESSENTIALS

SECURE ENTERPRISE joined with sister publication NETWORK COMPUTING for the mother of all firewall reviews—we tested 20 firewalls in four categories: Gigabit enterprise firewalls, XML gateways, branch-office firewalls and UTM (unified threat management) devices. The only vendor that submitted a single product in multiple categories was Secure Computing, which sent its 2150 model Sidewinder G2 for our gigabit enterprise and UTM reviews. Testing took place at our Green Bay, Wis., Syracuse, N.Y., Chicago and Gainesville, Fla., labs.

In the UTM category, we put five devices through their paces. Overall, we were underwhelmed. Although we told vendors we would test using publicly available exploits, only one product, ISS’ Proventia, detected everything. All the other devices let through at least one attack—even though the vulnerabilities we threw at them were at least a year old. Moreover, performance, especially with antivirus checking enabled, left much to be desired, and pricing was all over the map.

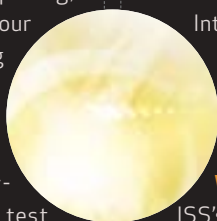
PRODUCT CATEGORY: UTM appliances, aka multifunction firewalls or all-in-one security appliances

MARKET DATA: By early next year, spending for all-in-one security appliances will exceed spending for specialized security devices, according to Gartner.

PRODUCTS TESTED: Fortinet’s FortiGate-800 Antivirus Firewall 2.8, Internet Security Systems’ Proventia M50 Integrated Security Appliance, Secure Computing Corp.’s Sidewinder G2 Security Appliance Model 2150 C 6.1, SonicWall’s SonicWall Pro 5060c and Symantec Corp.’s Symantec Gateway Security 5460

WHO WON AND WHY: Priced at a mere \$14,890, ISS’s Proventia detected every one of our attacks while providing decent management capabilities. Our main nit is that ISS could have made it easier to tune IDS/IPS features and antispam, antivirus, firewall and Web-filter capabilities.

WHAT HAPPENS NEXT: Check out the rest of our “Firewall Blowout” in the April 28 edition of NETWORK COMPUTING or at www.nwc.com, ID# 1608f1.



any case, those that didn't fare well will likely have fixes by the time you read this story. We scored protection capabilities, however, based on our initial set of attacks.

We then pulled together well-known virus files and sent them over FTP and SMTP with just names, no file extensions, to see if we could sneak any through. Every product except Secure Computing's Sidewinder offered antivirus scanning

The products that didn't fare well will likely have fixes by the time you read this story. The scores are based on our initial attacks.

of FTP traffic, and all the products successfully scanned e-mail attachments.

Signature updates are automatic for the most part, with many of the products able to update manually if necessary. A few of the firewalls required that we install firmware updates and perform reboots manually, but that's par for the course.

Yeah, But Can They Perform?

We get into the performance versus protection debate a lot. When a stateful packet-filtering firewall wins a review because of better performance, readers with application proxies flame

us, saying their firewalls provide superior protection. When an application proxy wins because of better protection, readers with the stateful packet filters rail that those other devices impact network performance. The right answer lies in the middle: We want good performance *and* strong protection.

Unfortunately, we discovered late that because of a series of errors, the tool we were using to test performance was misreporting results, and the testing scenario we wanted to create was radically different from the one we achieved. So much so that with less than 24 hours until press time, we decided to pull the performance results from this review. We couldn't develop and validate a test on such short notice, and we won't print misleading results. However, we can provide some general observations and post performance charts online (see www.secureenterprisemag.com/0205/0205f1.jhtml).

Antivirus scanning had a significant impact on overall firewall performance, for two main reasons. Before a firewall can scan files, it must queue them. Then it scans each file in turn and decides to send it, drop it or quarantine it. This process uses memory and introduces a high degree of "burstiness" as files are queued, scanned, and passed or dumped. In addition, virus scanning is CPU- and memory-intensive, and it degrades overall traffic performance. Some firewalls, in-

REPORT CARD / UTM FIREWALLS

	ISS Proventia M50 Integrated Security Appliance	Symantec Gateway Security 5460	Secure Computing Sidewinder G2 Security Appliance Model 2150 C 6.1	SonicWall Pro 5060c with SonicOS 3.0 Enhanced	Fortinet FortiGate-800 Antivirus Firewall 2.8
IDS/IPS					
TUNING (20%)	5	4	4	3	2
ATTACK DETECTION (15%)	5	3	2.5	2	1
ACTION PREVENTION (10%)	5	4	3	2	2
MANAGEMENT					
POLICY GRANULARITY (15%)	3	3	4	3	5
POLICY DEFINITION (10%)	3	3	3	4	4
REPORTING AND ALERTING					
DETAILS (10%)	4	3	2.5	2	2
CONFIGURATION (5%)	2	2	1	2	2
PRICE (10%)	4	2	2	4.5	4
UPDATES (5%)	4.5	4	4	4	5
TOTAL SCORE (100%)	4.13	3.40	3.08	2.90	2.85

A≥4.3, B≥3.5, C≥2.5, D≥1.5, F<1.5
A-C GRADES INCLUDE + OR - IN
THEIR RANGES. TOTAL SCORES AND
WEIGHTED SCORES ARE BASED ON A
SCALE OF 0-5.

ATTACK DETECTION is based on detecting attacks for well-known vulnerabilities and correctly naming them.

ATTACK PREVENTION scoring is based on vendor severity assessment and default settings. It also takes into account possible actions available.

POLICY GRANULARITY ranks the devices' ability to assign distinct IPS/antivirus/content-filtering rules.

POLICY DEFINITION ranks the configuration and management procedures for firewall rules and protection properties, including IPS tuning.

Note: Sidewinder tuning includes configuring application proxies like HTTP, SMTP and FTP.

Customize the results of this report card using the Interactive Report Card®, a Java applet, at www.secureenterprisemag.com.

cluding the FortiGate and Symantec Gateway Security, let you set antivirus configuration options on a per-rule basis, while others are more global.

Content filtering and IPS functionality generally have lesser, but still appreciable effects on performance. Each vendor defines *content filtering* differently. For one, it could be as simple as regulating MIME types, or going deep into files to search for key words in Web pages and e-mail. The more specific the content filtering, the slower the overall performance.

Making It Dance

So how configurable are these puppies? We're big fans of granularity—we like to tailor an appliance's protective features to our needs, not the other way around. Fortinet's FortiGate is a

model of fine-grained configurability. We could, on a per-rule basis, apply different sets of protection features, such as content filtering and antivirus scanning. That's handy when performance is a concern because you can enable advanced features as needed.

Once an appliance is processing lots of traffic, the management interface often slows to a crawl, rendering the device unmanageable. If you're brushing off this consideration, you've never tried to manage a firewall that was under DoS attack. We were happy to find that, even while under load, most of the devices remained manageable; the exception was the SonicWall appliance.

The clear winner in our review is ISS's Proventia M50. This \$14,890 champ caught all our attacks the first time and

TEST METHODOLOGY

When we set out to test unified threat-management appliances, we modeled our tests on real-world requirements. We laid out our network with a DMZ containing an SMTP MTA (message transfer agent), a DNS server and an HTTP server. Our internal zone housed our user clients and an Exchange Server. We designed firewall rules so that all traffic originating from the external zone went only to the DMZ, and all traffic originating from the internal zone could get to the DMZ and external zone. This is a common architecture. The bulk of our traffic originated from the internal zone.

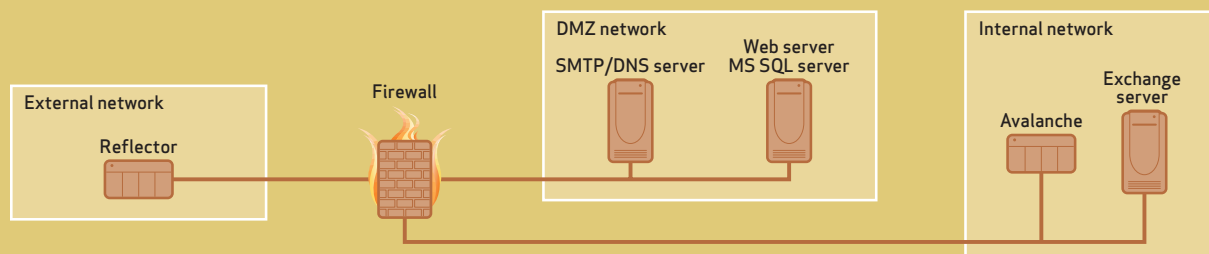
To test the protection features of the UTM devices, we used the Metasploit framework (www.metasploit.org) to attack vulnerable HTTP and SQL servers in the DMZ. We verified that the exploits worked prior to testing. We also used fragroute to fragment the traffic into 8-byte chunks to evade IDS detection. We then gathered up virus files, which we used for FTP and SMTP antivirus scanning. We set up the UTM appliances with similar policies to detect and block attacks and to detect and block viruses over SMTP and FTP, and we restricted access through the firewall, allowing only required services. We then tested each exploit and virus while the firewall was idle and while under load. We considered an attack properly detected and blocked if the UTM device named the exploit with a degree of accuracy. For example, several appliances named the ntdll.dll exploit as an overlong URI string, which is far too generic a classification to set a block on. If, however, the appliance named it, we attempted to block the attack. We notified vendors of the

results. We didn't change the grade if the IDS was properly configured but failed to detect or block the attack, even if the vendor issued a subsequent signature update.

Be careful with protocol parameters, such as maximum header and URL length in HTTP. Although we agree that it's unusual to have a URI longer than 100 characters, some longer ones are out there and there are longer headers. Be sure you understand the behaviors of your applications before you set arbitrary limits.

We strove to configure the firewalls with the strongest possible policy that would be similar across all the products tested so we could determine how the different feature sets compare with one another. Surprisingly, the core security features don't vary much. Some products add some nice touches, though. SonicWall's advanced protections are configured on zones, and you can enable antivirus and content filtering on a per-zone basis. Secure Computing and Symantec took that idea one step further, letting us configure advanced features on a per-rule basis.

All SECURE ENTERPRISE product reviews are conducted by current or former IT professionals in our Real-World Labs® or partner labs, according to our own test criteria. Vendor involvement is limited to assistance in configuration and troubleshooting. SECURE ENTERPRISE schedules reviews based solely on our editorial judgment of reader needs, and we conduct tests and publish results without vendor influence.



had adequate performance and management capabilities, earning it our Tester's Choice award. Symantec's Gateway Security and Secure Computing's Sidewinder G2 battled for the middle of the pack. Both cost more than double what the Proventia will set you back—\$36,700 and \$35,900, respectively—but each has strengths in application proxies, plus Symantec's offering is augmented with IDS/IPS while the Sidewinder's split DNS and SMTP proxies add a layer of protection to common protocols. Fortinet's and SonicWall's products brought up the rear; we were surprised at how poorly their offerings performed. The FortiGate missed three key attacks, while the SonicWall lacks rivals' policy granularity, has poor logging, underperformed with throughput and missed some key attacks.

ISS Proventia M50 Integrated Security Appliance

Internet Security Systems is a relative newcomer to the UTM field, but its solid experience in intrusion detection and vulnerability assessment have served it well: The Proventia was the only appliance to detect and name all the exploits we used, and really, that's the bottom line. In addition, the wealth of information Proventia provides about attacks and the causes is top-notch. However, its management interface leaves a lot to be desired. Navigating through screens was a challenge, and reporting was middle of the road.

ISS, like other vendors in this review, is conservative in enabling blocking on intrusion-detection rules—a wise stance. The Proventia has a wide variety of actions that can result from alerts, but the most common are blocking or resetting the connection and dropping the packet. Tuning IDS/IPS features—a requirement in nearly all IT shops—was needlessly complicated. We could tune default actions by entering adjustments on a per-signature or event-family basis through an advanced tab widget. For a few exceptions, this wouldn't be a problem, but for making wide-scale changes, it becomes another rule set to manage. ISS will make changes for you, but then you have to keep going back to the mother ship—not a scalable solution.



Proventia's IDS alerting provides a wealth of information to help admins understand the vital stats of an event and its impact.

Proventia's antispam, antivirus, firewall and Web-filter capabilities generally are enabled or disabled globally, with scant tuning available. For example, antivirus is enabled or disabled for HTTP, FTP, SMTP and POP3 globally. We prefer the granularity Fortinet provides, where profiles are applied on a per-rule basis.

Reporting was mixed. The Proventia logged data and provided excellent detail, which is especially handy when the IDS is firing off alerts. Being able to quickly absorb the particulars of malicious traffic let us immediately understand the risks and possible courses of action. However, the Proventia, like the other products we tested, cannot save filters for later reuse; we also couldn't create negate filters. Although we don't always know what we're looking for in a log file, we know what we don't want to see. Not being able to create a filter that says, "Don't show SYN Flood alerts," we had to slog through entries by hand.

Proventia M50 Integrated Security Appliance. Internet Security Systems, (800) 776-2362, (404) 236-2600. www.iss.net

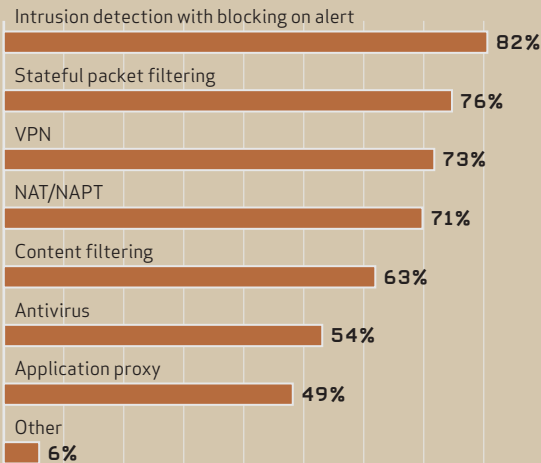
UTM FIREWALL ATTACKS

		Fortinet	ISS	Secure Computing	SonicWall	Symantec
Microsoft IIS 5.0 .printer ISAPI extension buffer overflow vulnerability	CVE-2001-0241	Allowed	Blocked	Blocked ²	Blocked	Blocked ²
Microsoft Windows ntdll.dll buffer overflow vulnerability	CAN-2003-0109	Detected ¹	Blocked	Blocked ²	Detected ³	Blocked ²
Unicode directory traversal	CVE-2000-0884	Blocked	Blocked	Blocked	Blocked	Blocked
Microsoft SQL Server user-authentication remote buffer overflow vulnerability	CVE-2002-1123	Blocked	Blocked	Allowed	Allowed	Allowed
Microsoft SQL Server 2000 resolution service stack overflow vulnerability	CAN-2002-0649	Allowed	Blocked	Allowed	Blocked	Allowed
Fragmentation evasion		No effect	No effect	No effect	No effect	No effect

¹Detected as a long URI, which may be a false positive, so we marked it allowed.
²Secure Computing's and Symantec's products are application proxies, and these attacks violate the HTTP protocol.
³Detected by 3 sigs (WebDAV access, overlong string and SQL injection attempt). All could be false positives.

READER POLL

What access-control features should a firewall have?



Multiple responses allowed

Source: NETWORK COMPUTING Reader Poll, 1,042 respondents

Symantec Gateway Security 5460 The Gateway 5460 is a blend of Symantec security products in a centrally managed appliance. The 5460 is unique because it features both application proxies (which inherently provide better protection against network- and service-level attacks and are also found in the Sidewinder) and intrusion-detection and -prevention functionality. However, its reporting is sparse and difficult to view at a glance; this is a recurring theme with Symantec's firewall. And, even given all its functionality, the 5460 is overpriced at \$35,900.

We've always maintained that application proxies, which fully support defined protocols like HTTP, SMTP or SQL*Net, offer better protection than stateful packet filters and even IPSs. This is because application proxies instantiate service protocols as a client and server. Service-level attacks typically violate protocols in some way, and we have shown in testing that they are best stopped by application proxies. However, there are two problems with this approach: The first is reduced performance, because of the increased processing and the additional latency required to set up a second connection completing the proxy. The second is that few application proxies are actually written. Common protocols HTTP, FTP, SMTP and DNS are easily found, but other common protocols, including Microsoft SQL, use generic proxies that do nothing more than proxy TCP and UDP connections.

The 5460 addresses the second shortcoming with its IDS/IPS feature, which triggers on malicious traffic per an attack-signature match. An interesting phenomenon on the 5460 is that the IIS .printer and ntdll.dll overflow attacks were detected and blocked on the application proxies, not processed by the IDS. The Unicode attack was passed through the application proxy because it is valid HTTP traffic, but it triggered an IDS alert. That's what we call an interesting pairing of comple-

mentary technologies. Unfortunately, because Symantec doesn't have an application proxy for SQL Server and no signatures for the two well-known exploits we used, our SQL Server overflow attack was not caught.

Firewall rule and configuration changes were often a multi-step process, where we had to apply changes and then save them to the firewall. If we forgot the second step, our modifications didn't take effect. Application proxies are configured on a per-rule basis, so as with the FortiGate, we could tailor protective mechanisms as needed.

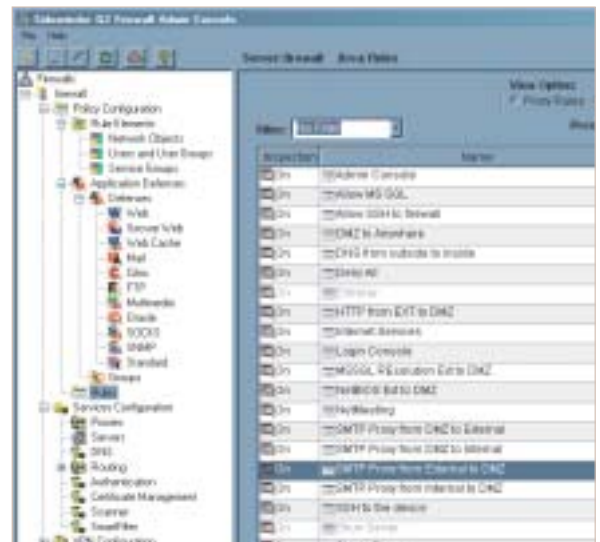
Logging, while detailed, was rather awkward to use, which is the last thing you want to deal with when troubleshooting. The logging system had filtering capabilities, but again, we found no way to define a negate filter.

Symantec Gateway Security 5460. Symantec Corp., (800) 441-7234, (408) 253-9600. www.symantec.com

Secure Computing Sidewinder G2 Security Appliance Model 2150 C 6.1

The Sidewinder, like Symantec's Gateway Security, is an application proxy firewall, except it doesn't support signature-based intrusion detection and prevention. Rather, Secure Computing focuses on building application-level proxies. Content filtering and antivirus are added protections. We did nick Secure Computing on attack detection because of its lack of integrated IDS and antivirus scanning on FTP traffic. Byte for byte, an application proxy provides better protection than an IPS, but as we found with Symantec Gateway Security, the IPS can fill gaps in application-proxy coverage. We'd like to see Secure Computing close some of those gaps.

The Sidewinder is highly tunable; we're impressed with the options available in configuring application proxies. Different



The Secure Computing Sidewinder's Java-based administration console takes some getting used to. The rules section lists all rules available for a policy, but the Active Policy must be viewed separately.

profiles can be defined for an application defense, which is then used to configure protection features. For example, we created an HTTP profile of the enforced content control and allowed only the *get*, *post* and *head* methods. We also disallowed Unicode encoding in the URI. We could then apply that profile to a rule. But not all application-defense mechanisms had as many options as HTTP.

The Sidewinder achieves high performance for an application proxy by limiting the amount of resources it expends on application inspection. Normally, application proxies must move network transactions from the NIC up into user space, proxy the traffic to the “other side” and send it back down to the NIC, creating a bottleneck. Secure Computing changed how the Sidewinder proxies traffic, setting it to inspect only packets that require protocol analysis. For exam-

ple, if a Web client is doing an HTTP *get*, only the first few packets must be inspected. Once the *get* is successful, the rest of the transaction is just moving data, which is kept in kernel space and requires much less overhead. This intelligent inspection provides the best of both worlds—application proxy and good performance.

Still, these benefits don’t justify the high price, and like the Symantec Gateway Security, logging left lots to be desired. Although there were plenty of details, ferreting out the salient ones took more mental processing than we like to expend on parsing logs when troubleshooting or even monitoring the firewall.

Sidewinder G2 Security Appliance Model 2150 C 6.1. Secure Computing Corp., (800) 379-4944, (408) 979-6572. www.securecomputing.com

UTM FIREWALL FEATURES

	Fortinet FortiGate-800 Antivirus Firewall 2.8	ISS Proventia M50 Integrated Security Appliance	Secure Computing Sidewinder G2 Security Appliance Model 2150 C 6.1	SonicWall Pro 5060c with SonicOS 3.0 Enhanced	Symantec Gateway Security 5460
Number of interfaces supported					
Fast Ethernet	4 10/100 Base-T ports	8	6 to 14	None	Up to 8
Gigabit	4 10/100/1,000 Base-T ports	8	6 to 14	6	Up to 8 [Fiber Gig available]
Third-party supplied (or internal) engine or signatures					
Antivirus	Internal	Sophos AU	McAfee	Undisclosed	Internal
Content filtering	Internal	Internal	SmartFilter [Secure Computing]	BlueCoat	Internal
Spam filtering	Internal	Internal	Cloudmark	Undisclosed	Internal
Intrusion detection	Internal	Internal	None	Internal	Internal
Protection features					
Firewall	Y	Y	Y	Y	Y
VPN	Y	Y	Y	Y	Y
Intrusion detection (signature)	Y	Y	N	Y	Y
Intrusion prevention (signature)	Y	Y	N	Y	Y
Antivirus	Y	Y	Y	Y	Y
Content filtering	Y	Y	Y	Y	Y
Antispam	Y	Y	Y	Y	Y
Antivirus protocols	FTP, HTTP, IMAP, POP3, SMTP	FTP, HTTP, POP3, SMTP	HTTP, SMTP	FTP, HTTP, IMAP, POP3, SMTP, TCP-stream-based protocols	FTP, HTTP, SMTP
Updates					
System firmware: manual or auto	Both	Both	Both	Both	Manual
Signatures: manual or auto	Both	Both	Both	Both	Auto
Logging	Internal and external logs, can log to FortiLog	Internal logs, event logging, e-mail, SNMP, central management	Internal and external logs	Internal and external logs, SonicWall Global Management System, ViewPoint Reporting, NetIQ Firewall Suite, others	Internal logs, remote log extract tool
Alerting	E-mail, management UI, SNMP traps	E-mail, management UI, SNMP traps	E-mail, management UI, SNMP traps	E-mail, management UI, SNMP traps	E-mail, management UI, SNMP traps
Price	\$11,995	\$14,890	\$35,900	\$10,995	\$36,700

Y=Yes, N=No

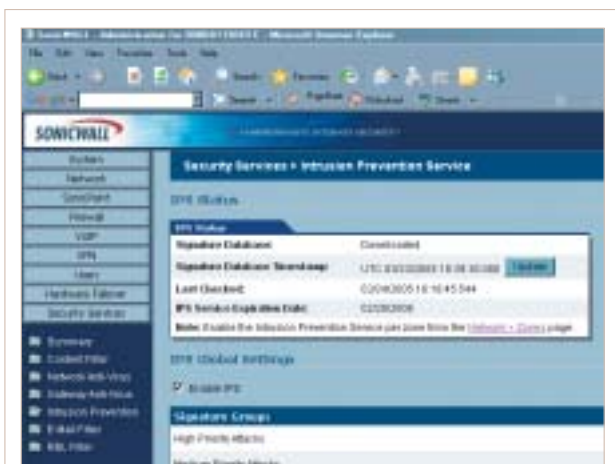
SonicWall Pro 5060c with SonicOS 3.0 Enhanced

The inexpensive SonicWall 5060 seems to be targeted at a midsize companies. In our first round of attacks, the device detected three out of five exploits and, like ISS's Proventia, wasn't thrown by our fragmentation evasion attempt. The SonicWall did detect our ntdll.dll exploit, but it failed to name the attack properly, which would have led us to believe it was a false positive. The device's policy definitions weren't as granular as Fortinet's, and its IPS responses were not even close to those offered by ISS. As a firewall, the SonicWall is solid, but we're not convinced the device's intrusion-detection capabilities are up to snuff.

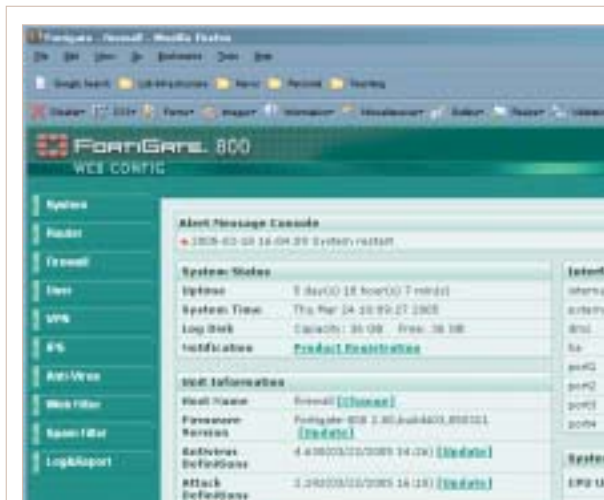
Once we had the SonicWall installed and the firewall policies configured, we enabled the IPS on the LAN zone and the DMZ zone. We fired off our attacks, and four triggered alerts. Only three, however, were correctly identified. The Microsoft SQL Server buffer flow attack passed unnoticed, and the Windows ntdll.dll overflow triggered three different alarms: one for WebDAV access, one for an over-long URI and one for a SQL injection attempt that left us scratching our heads. None of these would have indicated that someone was attempting to exploit a two-year-old vulnerability. To make matters worse, these exploit signatures were all marked as low priority. We told SonicWall about our results and the company updated its signature databases within the week.

The SonicWall's alert logs are filterable, and when we clicked on an IPS event, we could edit signature properties, such as default action. There's also a link that took us to more information about the event. Unfortunately, the SonicWall doesn't log traffic that passes through allow rules, except through syslog or SonicWall's Viewpoint reporting software. Makes troubleshooting a bit difficult.

We also found that while under load, the SonicWall was essentially unmanageable. Sure, we were managing the Son-



The SonicWall Pro's ubiquitous Web interface doesn't change much, whether you're looking at the little TZW or the 3060. Security services, like IPS, can be configured either on a global, group or individual level.



The Fortinet FortiGate-800's status page summarizes the health of the firewall at a glance. The CPU meter shows high utilization while testing, and the content summary rolls up common protocol usage.

icWall from the same interface traffic was arriving on, but we never got above 50 percent utilization during our tests, so management shouldn't have been degraded because of high traffic.

SonicWall Pro 5060c with SonicOS 3.0 Enhanced. SonicWall, (888) 557-6642, (408) 745-9600. www.sonicwall.com

Fortinet FortiGate-800 Antivirus Firewall 2.8

Fortinet markets the FortiGate-800 as a high-speed antivirus gateway. Add in the IPS, content filtering and anti-spam capabilities, and you get the whole enchilada. But FortiGate's reporting, a critical feature in security gear, is subpar. We also were sorely disappointed with the device's intrusion-detection capabilities: The FortiGate properly detected only two of the five attacks we threw at it.

The FortiGate does have some redeeming qualities. It is easy to configure and its rule set is highly readable. We also like the system status page, which was unique among the devices tested and gave a quick overview of the firewall. We configured and applied different protection profiles on a per-rule basis, so we could customize traffic protections. For example, we applied a restrictive content-filtering and antivirus profile for one rule, and a less restrictive set of rules for another. Logging is sparse, barely giving enough details to troubleshoot problems. However, unlike the SonicWall, we could log all traffic, and the FortiGate has a modular system for determining what gets reported.

Fortinet FortiGate-800 Antivirus Firewall 2.8. Fortinet, (866) 868-3678, (408) 235-7700. www.fortinet.com

MIKE FRATTO



is editor of SECURE ENTERPRISE. He was previously a senior technology editor for NETWORK COMPUTING and independent consultant in central New York. Write to him at mfratto@secureenterprisemag.com.