

## Cover Story

---

### Unify Network Protection

*Simplification of network security, by combining multiple security functions in one box, is the main selling point of unified threat management appliances.*

*by Robert Smithers and Martin Milner*

Companies considering deploying unified threat management (UTM) technology have various offerings and approaches to consider, with many different products to address specific network requirements. The lure of UTM is strong as companies and their network administrators struggle to cope with ever-intensifying security threats while battling IT hardware and software sprawl. Vendors of UTM appliances contend their all-in-one approaches offer more comprehensive protection, easier management and better return on investment than do standalone security applications.



To meet the definition of a UTM appliance for testing by Miercom, a device needed

to include a stateful firewall (FW), intrusion detection (IDS), some form of intrusion prevention (IPS), antispam (ASP) and antivirus (AV). The appliances needed to be capable of running all these functions simultaneously.

Miercom reviewed appliances from four vendors: the FortiGate 3016B from Fortinet ([www.fortinet.com](http://www.fortinet.com)), the SSG-550 from Juniper Networks ([www.juniper.net](http://www.juniper.net)), the NSA E7500 from SonicWALL ([www.sonicwall.com](http://www.sonicwall.com)) and the Firebox Peak X 8500e UTM Bundle from WatchGuard Technologies ([www.watchguard.com](http://www.watchguard.com)). These vendors were chosen because they offer complete UTM security solutions for the enterprise market, as well as a significant market share.

Testing focused on both the effectiveness of the UTM appliance as well as performance throughput. The tests were designed to stress the filtering capabilities of the appliances and determine how these countermeasures impacted network throughput. An assessment of the different capabilities and differences between products included the number of nodes supported, the types of security provided, whether firmware upgrades were allowed, and advanced feature sets.

The UTM appliances tested approach threat detection in unique ways. They each differ in how they integrate the components of UTM, how easily policies are able to be configured and modified, and in the clarity of the management reporting and monitoring of traffic.

Performance testing consisted of throughput capability analysis, using an XM12 load generator from Ixia ([www.ixiacom.com](http://www.ixiacom.com)), and threat-blocking analysis, using both a BreakingPoint Systems ([www.breakingpointsystems.com](http://www.breakingpointsystems.com)) BPS-1K security appliance and a MuDynamics ([www.mudynamics.com](http://www.mudynamics.com)) Mu-4000 multiprotocol testing appliance, together with Miercom's in-house suite of vulnerability and threat analysis scripts and defeat techniques compiled over the last 20 years of testing network products.





The BreakingPoint system delivered a strike level 5 test that included exploits, network worms, denial-of-service attack, reconnaissance attacks, Trojan horse and backdoor intrusions.

The MuDynamics unit tested the ability of the system under test (SUT) to protect a network from threats with published threat signatures even before patches are applied. Mu's Published Vulnerability Analysis (PVA) suite evaluates the ability of the SUT to protect against vulnerabilities rather than exploits, checking for currency and traffic patterns that may identify a new threat.

The UTM effectiveness tests produced data to confirm the SUTs perform the functions expected of them. The effectiveness of blocking attacks was the goal of this component of the review. Throughput handling was measured in a separate component of this review to gauge the capacity of these systems.

What counts most in deploying UTM technology is how fast the device works when all services are activated. The tests proved that activation of services—antivirus in particular—slowed throughput substantially. Finally, the appliances' management and administration interfaces were analyzed for effectiveness and intuitiveness in design.

## Features Compared

	<b>FORTINET FortiGate 3016B</b>	<b>JUNIPER NETWORKS SSG-550</b>	<b>SONICWALL NSA E7500</b>	<b>WATCHGUARD Firebox Peak X 8500e UTM bundle</b>
				
<b>Security services</b>	IPS/IDS, AV, ASP, FW; CS	IPS/IDS, AV, ASP, FW; Web Filtering	IPS/IDS, AV, ASP, FW	IPS/IDS, AV, ASP, FW. URL filtering
<b>Suitable for</b>	Large enterprise, service provider networks and data centers	Regional and branch office deployments, medium-sized enterprise	Distributed, campus environments and data centers	SMEs with growing networks, main office/HQ
<b>Number of users</b>	Unlimited	Unlimited	2,500	800-3,000+
<b>Protects against</b>	Content and network-based threats, including 3,000 known threats	Viruses, spam, unauthorized Web use, including worms, Trojans and backdoor attacks	Content and network-based threats, including up to 3,000 known ones; DoS/DDoS and scanning attacks	Spyware, Trojans, viruses, buffer overflows, SQL injections, instant messaging and P2P usage policy violations

## Strengths & Weaknesses

<b>Strengths</b>	<p>Clear, concise management interface</p> <p>Web GUI's status page showed number of viruses caught and intrusions detected</p> <p>Consistent throughput numbers with all services enabled</p> <p>Redundant power supply</p>	<p>Best throughput performance across-the-board regardless of services enabled</p> <p>Redundant power supply</p>	<p>Expandable chassis that contributes to scalability</p> <p>Redundant power supply</p>	<p>Proxy-based filtering is most effective at blocking malicious traffic</p> <p>Well-designed front-panel display</p>
<b>Weaknesses</b>	<p>Lower overall throughput when all services enabled</p> <p>Virus detection requires AV policy be turned on in all network directions, not just the direction virus is coming from</p>	<p>Throughput not consistent with all services</p> <p>Time-consuming method to search through logs for detected intrusions</p>	<p>Unreliable management interface for upgrading firmware and signatures</p> <p>Non-intuitive, disorganized deep-packet inspection setup</p>	<p>Single power-supply does not provide on-device redundancy</p>

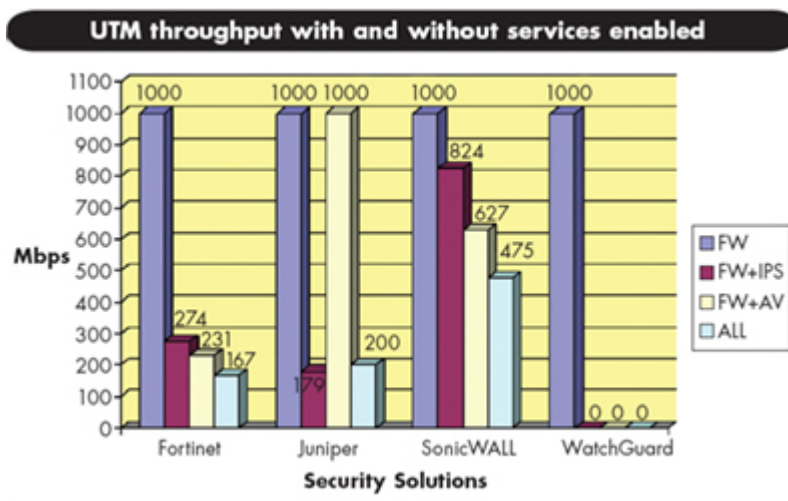
The four UTMs were far from plug and play, with some frustrating snags and glitches cropping up during the installations. Some of the administration interfaces were difficult to use and would likely inhibit effective UTM device deployment.

Comprehensive security provision is asking a lot of one box, especially at enterprise-level demand. Three of the four tested units failed to block many of the security threats delivered by the three security effectiveness test systems. The Watchguard Firebox Peak X 8500e was the exception and performed well on all security effectiveness tests.

The SonicWALL NSA E7500 handled network traffic both with and without all countermeasure features enabled. Since none of the devices tested stopped all threats, nor could produce full line rate network protection, enterprises might want to consider employing separate network and endpoint security applications.

## Fortinet FortiGate 3016B

Fortinet's FortiGate 3016B was introduced in 2007 as an expansion of the company's FortiGate 3000 series UTMs or, as Fortinet calls them, "multithreat security appliances." The 3016B was designed to be highly scalable and capable of delivering up to 26 Gbps of firewall performance with optional expansion modules installed.



The graph shows how throughput diminishes when UTM services are progressively turned on. Firewall-only throughput was capped at 1 Gbps, a level reached by all tested units.

**Notes:**

*All: Six interfaces were used.*

*WatchGuard: When all services were enabled the device treated all of the Ixia-generated traffic as a denial-of-service attack, blocked everything and prevented a valid reading. Settings need to be tweaked.*

*Juniper: The anomalous gateway antivirus results shown were due to antivirus policies that were not enabled for all zones. When AV profile was enabled for all network zones, appliance memory usage went to approximately 100 percent and throughput dropped to zero.*

It includes FW, IPS/IDS, AV and ASP. The 3016B has two built-in copper Gigabit Ethernet ports and 16 SFP interfaces, of which two can be fiber. For survivability, the 3016B is hot-swappable, with redundant power supplies and fans.

The Fortinet's administration and management offerings include a single-screen, Web-based user interface, command-line interface and console interfaces, as well as telnet secure shell (SSH). The management is role-based, with multilanguage support and multiple administrator and user levels. Management can be centralized using Fortinet's FortiManager.

The system breaks down capture information into number of viruses per IPS detection. This means users need not consult logs to get that information. It sends logs to Syslog and/or a Web-Trends Enhanced Log File (WELF) server.

The UTM provides graphical historical and real-time reports and can send virus and attack information via e-mail. Logging information is accomplished with Fortinet's FortiAnalyzer.

Fortinet uses a protection profile. Once created, that profile can be assigned as a name to various zones. This eases the implementation of the same policy across multiple network zones.

The 3016B shows administrators the date of the last virus signature update. Signatures are updated daily. The Fortinet UTM's IPS protects against more than 3,000 known threats and includes protocol anomaly analysis. Out of the box, the appliance is set to let all traffic pass, leaving the user to specify which types of traffic are blocked (via packet filtering).

To boost the Fortinet FortiGate 3016's speed, Fortinet paired its FortiASIC-CP6 Content Processor with a new network processor called the FortiASIC-NP2. To enable even faster speeds, particularly for use in time-sensitive applications, such as voice-over Internet protocol (VoIP), Fortinet offers hardware-accelerated Gigabit Ethernet interfaces.

During the performance tests, the 3016B achieved 324 Mbps with the stateful firewall enabled. It was tested using only six of its 18 available interfaces and without expansion modules installed. The SUT could possibly have achieved higher throughput if additional interfaces were utilized and the load

distributed; however, the tests needed to remain consistent with the number and types of interfaces in this review.

The UTM provided 274 Mbps when IPS was activated with the firewall enabled, 231 Mbps when the IPS was turned off and the gateway antivirus was activated, and 167 Mbps when the firewall, the IPS and the antivirus were running simultaneously.

The Fortinet FortiGate 3016B blocked 92 percent of the threats generated by a MuDynamics PVA test and 44 percent of those by the BreakingPoint.

## **Juniper networks SSG-550**

The SSG 550, part of Juniper's SSG 500-series UTMs, is marketed as a security platform for large regional branch offices and medium-sized businesses. It supports up to 256,000 concurrent sessions and 15,000 new sessions per second.

The appliance uses stateful firewall, Internet protocol security (IPSec), VPN, IPS, AV, ASP and Web filtering to shield against worms, viruses, Trojans, spam, phishing, adware and malware. The Juniper UTM allows administrators to create up to 60 separate security zones, independent secure domains with distinct policies that can include access control rules.

Juniper requires the creation of policy rules for each network zone individually and manually. Administrators can designate which UTM security features are used in each zone. The SSG 550 administrator also has the ability to set up 150 virtual LANs and eight virtual routers.

The Juniper appliance provided the most connectivity and scalability options of the four tested. The SSG-550 has four onboard 10/100/1,000 interfaces and six I/O expansion slots for LAN or WAN interfaces. The SSG-550 provides policy-based and product lifecycle management.

The system allows command-line input via console or telnet, as well as a graphical Web-based user interface for HTTP and HTTPS. Netscreen Security Manager can provide centralized management.

An array of alarms, emergency alerts, errors and warnings are provided. The appliance can be linked to the Web for automatic updates or threat signatures can be downloaded from Juniper's Web site and updated locally.

Intrusion detection and prevention is enabled with an annually licensed IPS engine with Juniper Deep Inspection Firewall signature packs. These packs allow users to tailor the attack protection to specific types.

The Juniper UTM is designed to allow all traffic except for that defined by the administrator as being a threat. While this protection strategy allows higher network throughput, it does so at the cost of some network security.

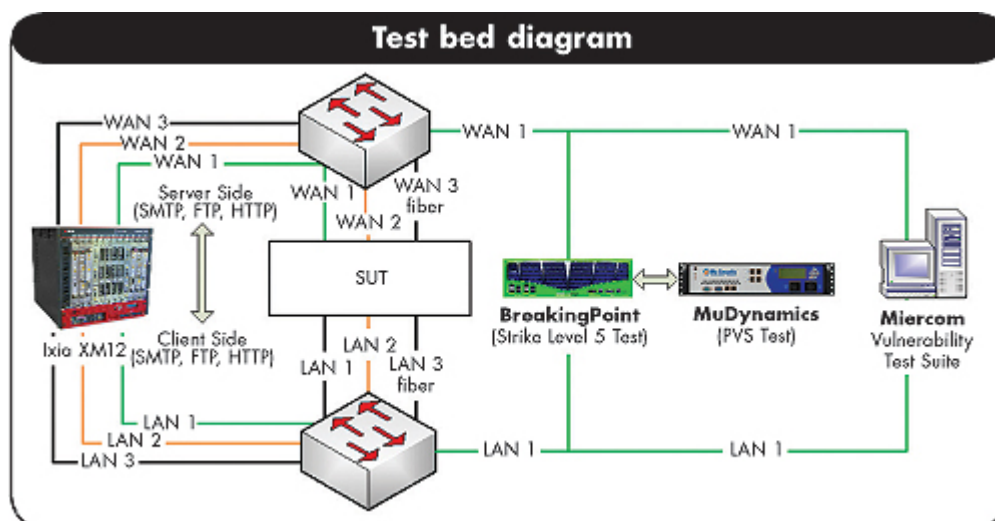
During the test, the unit reached 179 Mbps with the firewall and IPS enabled. When IPS was turned off and AV activated, the SSG-550 throughput hit 1 Gbps, but only when antivirus policies were turned off for some zones.

The SSG-550 was the only UTM not capable of scanning the 200 Mb AV-testing files generated as part of Miercom's own testing suite. The box could scan files under 30 MB without difficulty but could not deal with files larger than 30 MB. The SSG-550 blocked 48 percent of the threats generated by the BreakingPoint security appliance.

## SonicWALL NSA E7500

SonicWALL's enterprise-class Network Security Appliance (NSA) E7500 relies on 16 parallel performance processing cores. The device, capable of handling 2,500 users, one million concurrent sessions and 25,000 new sessions per second, is marketed for use in campus networks, distributed environments and data centers.

SonicWALL credits the NSA E7500's multicore design with the system's throughput speed capabilities. The unit is capable of reaching up to 5.6 Gbps throughput with the firewall enabled, 2.58 with IPS, 1.85 Gbps with antivirus and 1.7 Gbps general UTM throughput.



The E7500 includes IPS and IDS, AV, ASP, FW and URL filtering. The UTM is designed to protect against spyware, Trojans, viruses, buffer overflows, SQL injections, instant messaging and peer-to-peer (P2P) file usage policy violations.

SonicWALL approaches the creation of policy rules for network security zones from more of a building-block basis, wherein network administrators create objects, assign the objects to a group and then assign a policy that incorporates those group elements.

The E7500 comes with four Gigabit Ethernet copper interfaces, four high-speed configurable small form-factor pluggable (SFP) ports, one Gigabit Ethernet high-availability port and secure wireless LAN functionality. The unit supports up to 512 VLANs.

Threat signature updates for the NSA E7500 are provided daily over the Internet, provided the UTM's license is current. This is checked automatically during log-in, and the application of new signatures is also automated.

The SonicWALL's intrusion detection and prevention abilities include digital rights management, P2P and instant messaging controls. The box shields against up to 3,000 known content- and network-based threats and against 22 classes of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. Survivability is provided by redundant hot-swappable power supplies and fans. The E7500 is a fixed configuration and is not expandable.

Administration and control of the SonicWALL UTM is provided by the vendor's Global Management System (GMS), providing a number of tools to centrally manage the NSA E7500 across distributed enterprises. It presents real-time monitoring metrics, allows for integration of policies and for compliance reporting. Command-line input and console access are also offered and captured information is entered to a time-stamped log.

Miercom lab tests found the appliance attained the desired 1-Gbps throughput with stateful firewall enabled. When the IPS and the firewall were turned on, the box managed 824 Mbps. Switching off the IPS and activating the antivirus yielded a throughput of 627 Mbps, and turning on the firewall, the IPS and the antivirus brought the throughput down to 475 Mbps.

The E7500 blocked 99 percent of the threats generated by a MuDynamics PVA test and 50 percent of those by the BreakingPoint.

## **WatchGuard firebox bundle**

The Firebox X Peak line is WatchGuard's high-performance collection of UTM appliances. The X 8500e tested came in a UTM bundle, a package that includes everything needed for comprehensive network protection.

The Firebox X Peak 8500e is marketed as a security solution for growing small- to medium-sized enterprises with 800 to more than 3,000 users, one million concurrent sessions and 6,200 new

sessions per second. It has eight Gigabit Ethernet interfaces, supports 400 VLANs and allows administrators to configure eight separate security zones. Any of the eight ports can be configured as internal, external or optional.

WatchGuard's UTM bundles include FW, VPN, IPS, URL filtering, AV and antispyware. The WatchGuard approach to security is different than the others in this review. Using proxy-based technology, all traffic is blocked except for that allowed by the network administrator. This system provides the most security since all traffic is treated suspect and not allowed to enter the LAN, preventing the propagation of threats. This approach results in slower throughput but offers stronger security.

The 8500e is capable of identifying and blocking emerging threats, providing automatic protection from spyware, Trojans, worms, DoS, DDoS, DNS poisoning, buffer overflows and other attacks. The appliance also can identify and block threats that arrive on non-standard and non-assigned ports.

WatchGuard uses a thick client to administer the box. Firewall policies can be either packet-filter based or proxy-filter based, and are configured with a policy manager.

During the throughput testing, the 8500e interpreted a massive amount of data sent by the Ixia over six ports as a DoS attack, and immediately blocked all traffic. It also blocked 97 percent of the threats generated by a MuDynamics PVA test and 99 percent of those by the BreakingPoint.

To provide zero-day attack protection—meaning the blocking of threats as soon as they are launched, and before they have been identified and included in the signature databases—WatchGuard uses protocol anomaly detection (which turns away traffic that does not conform to established protocol standards), pattern matching (blocking risky files by fully inspecting the whole packet) and behavior analysis (to derail traffic coming from sources that are acting suspiciously).

*Robert Smithers is the CEO and Martin Milner is a senior researcher at Miercom, East Windsor, N.J. Miercom will continue this industry assessment of security products into 2009, with results appearing in Communications News. Companies may submit a unified threat management product to Miercom to be independently indexed in this industry assessment at no charge. Phone: 609-490-0200 [rsmithers@miercom.com](mailto:rsmithers@miercom.com) [www.miercom.com](http://www.miercom.com)*

For more information ([click here](#))

---

## Comments

## **Add a Comment**

Comments will be proofed by editorial before being posted live. This may take up to one business day.

Name