IDG .com

NETWORKWORLD® Reprint

The leader in network knowledge ■ www.networkworld.com April 7, 2008 ■ Volume 25, Number 14

SonicWall smashes UTM gigabit speed barrier

New appliance offers enterprise-level UTM performance

BY JOEL SNYDER, NETWORK WORLD LAB ALLIANCE

In March, SonicWall rolled out its next-generation unified threat-management firewall appliance geared for the enterprise. The results of our exclusive test of the Network Security Appliance E7500 show that SonicWall indeed has crashed through the speed barrier.

This box offers 1.3Gbps of UTM performance, which is nearly triple the speed of the fastest product in our comparative UTM test last November (See "Testing all-in-one firewalls," www.nwdocfinder.com/4321).

While SonicWall has not changed much on the surface of its firewall, there are dramatic differences in its internal architecture that yield performance gains that leapfrog the throughput numbers of the SonicWall Pro product line. This makes UTM features — intrusion-prevention system (IPS), antivirus, antispyware and content filtering — cost-effective because they can run at gigabit speeds.

Fifth-generation multicore performance

SonicWall's NSA firewall line is based on a family of multicore security processors from Cavium. The new hardware (six models have been announced) is slated to replace the company's Pro series.

The high-end E7500 we tested has a 16-core Cavium CPU, with each core operating at 600MHz. One core is dedicated to system management, and the rest are used for security processing, including firewall; VPN and other UTM features, such as antivirus, IPS and content filtering. Also built into the CPU is hardware acceleration for cryptography (useful in VPNs); compression; and regular expressions, which compare a pattern against a string, and are heavily used in most IPS rule sets.

The E7500 is a 1U, short (16-inch), rack-mountable device with eight firewall ports: four copper Gigabit Ethernet interfaces and four Series-1 Port gigabit interfaces. An additional port is marked for high-availability connectivity to another firewall. The E7500 also has redundant, hot-swappable fans and power supplies. Drawing 0.9 amps when unloaded (and 1.1 amps when fully loaded), the E7500 is a middle-of-the-road power consumer for an appliance of its size.

We tested the E7500 by putting it through performance tests very similar to those we used in our previous UTM test. (See "How we did it," page 2). To drive the E7500 to its UTM limits, however, we used a faster set of Spirent Communications WebAvalanche and WebReflector test devices.

Full UTM performance (including client and server-side IPS signatures, antivirus, antispyware and content filtering) was 1,288Mbps using recommended settings. For comparison, the fastest fully loaded UTM performance registered in our earlier test was by the Fortinet FortiGate 3600A, which came in at 520Mbps.

SonicWall's Network Security Appliance line pushes UTM performance.

NETRESULTS

Product	**SonicWall NSA E7500 Version 5.0**
Vendor	SonicWall www.sonicwall.com
Price	$25,000
Pros	Very high-performance UTM features; small size; low power consumption; high interface density; redundant power supplies and fans; SonicPoint wireless LAN management system and wireless IDS
Cons	Manageability of UTM features limited, especially in IPS; Web-based management system had difficulty handling complex policies in firewall or NAT; firewall configuration flexibility held back by built-in configuration limits
Score	**4.01**

SCORECARD

Action	Weight	
Performance	25%	**4.75**
Intrusion prevention	15%	**2.50**
Antivirus	15%	**4.50**
VPN	15%	**4.00**
Management	15%	**3.50**
Hardware architecture	10%	**4.50**
Power	5%	**4.00**
Total score		**4.01**

Scoring key: 5: Exceptional; **4:** Very good; **3:** Average; **2:** Below average; **1:** Subpar or not available.

© Copyright 2008 by Network World, Inc., Southborough, MA 01772-9108 • Posted from Network World • Trademark is owned by International Data Group, Inc.
#1-23883883 Managed by The YGS Group, 717.399.1900. For more information visit www.theYGSgroup.com/reprints.

Tracking SonicWall UTM performance

The NSA E7500's UTM results set a new bar for UTM-firewall price and performance. With full UTM scanning at 1.3Gbps, SonicWall has an enterprise-speed product in a pint-size box.

	Performance* with only AV enabled	Performance* with only IPS enabled	Performance* with AV, IPS, antispyware and content filtering enabled
Using recommended settings	1615	1914	1288
Using maximum security setting **	1609	1221	848
Using performance-optimized setting	1937	1921	1867

*in Mbps ** This setting option will be eliminated in future firmware versions of this product.

Although firewall vendors upgrade their wares constantly, SonicWall is the first with a major leap past the gear we tested previously.

We had similar results when we tested IPS performance on the E7500 (1914Mbps using recommended settings) and antivirus performance (1615Mbps using recommended settings); both were significantly faster than the best numbers of the high-end gigabit products in our earlier test. Compared with SonicWall's own previous top-of-the-line Pro 5060, the results are even more dramatic, with the E7500 coming in six to eight times faster in all UTM tests.

Overall, the E7500 provides a dramatic boost in speed that makes UTM possible in enterprises needing gigabit speeds.

User interface remains the same

The E7500's hardware changes are hugely evident in its performance numbers, but its Web-based user interface (which most enterprise network managers will find to be easy to learn) and the underlying firewall feature set are little changed from what we saw in our previous test.

The strong extra features for which SonicWall products are known — such as wireless LAN management system, wireless intrusion-detection system, VoIP using Session Initiation Protocol support, and high-end diagnostic tools — are still there and haven't changed significantly from previous versions.

One new feature is that IT can change the scanning parameters for UTM features between the "Recommended" and "Performance Optimized" settings. A third setting called "Maximum Security" also was included in the firmware we tested, but it will be removed from the next version. SonicWall engineers say they are making the change because the level of security in the "Recommended" and "Maximum" settings was actually the same. SonicWall told us (the feature is so new it isn't in the documentation yet) that this doesn't turn on and off signatures in the IPS or antivirus parts of the product, but rather optimizes how it scans to look for the most common threats. In our performance testing, we saw some fairly dramatic speed differences when we employed the various security settings (see graphic, above).

The higher performance of the E7500 on UTM tasks also led us to upgrade its overall IPS score. The management and coverage of the E7500 IPS is largely unchanged from that in Version 4 of the SonicWall software.

The E7500 still shows signs of SonicWall's small-and-midsize-business heritage. So, while some features, such as IPS, are now extremely fast, SonicWall hasn't done much to improve the manageability or control of the firewall or the UTM feature set. For example, it's still very difficult to tune the IPS to suppress an alert for a particular system, and tuning produces a nearly unmaintainable configuration. Similarly, you still cannot have separate UTM configuration sets for different zones or different flows through your network. The result is that this firewall is capable of handling an immense amount of traffic, but it fits best into networks where all the traffic should be handled the same way.

If you already love the SonicWall interface and features, the E7500 will be a great way for you to boost performance. On the other hand, if you were unhappy with SonicWall's feature set or management system before, the E7500 won't give you any reason to change your mind.

Bottom line

SonicWall has garnered tremendous loyalty from its customer base by offering network managers a UTM feature set at a competitive price. One of the Achilles' heels of the product line, however, has always been its UTM performance. With the E7500, SonicWall takes its firewall products up to enterprise speeds.

Snyder is a senior partner at Opus One, a consulting firm in Tucson, Ariz. He can be reached at Joel.Snyder@opus1.com.

How we did it

We evaluated the SonicWall E7500 using the same criteria we used in our November 2007 test of unified-threat-management products. Because the main changes in the firewall were in its performance capabilities, we focused on performance testing.

To test performance, we used Spirent Communications' WebAvalanche 2700 and WebReflector 2700 test appliances to generate HTTP traffic across the E7500. We set up a profile using a typical Internet mix of traffic ranging in size from 1KB objects to 1.5MB objects, and ran HTTP transactions through the firewalls. Because we were using only four ports on the firewall (two for clients and two for servers), the maximum speed we could measure would be 2Gbps. It is possible that some of our performance measurements above the 1920Mbps range do not measure the maximum performance of the E7500 adequately, because the performance could have been constrained by line speed rather than system capability.

Initially, we had difficulty getting consistent performance results from the E7500 in our lab. Over two months, we replaced not only the E7500 but also the firmware, the infrastructure switches, and our WebAvalanche and WebReflector systems. We finally got consistent results but couldn't isolate the cause of the inconsistent results. All our final tests were done using Version 5.0.0.10-e of the firewall firmware.

We also discovered that the performance of the E7500 can vary depending on what types of traffic were used in testing. Like a soft-ripened cheese, you see very different textures depending on what angle you slice at. For example, when we skewed the types of traffic that the E7500 was scanning to have a mix — including HTML, ZIP, Microsoft Word, Windows executables and several image types — that was very different from our "normal" Internet distribution, we saw dramatic performance differences in antivirus and intrusion prevention. In some cases, performance went up, and in others it went down. While we found the E7500 to have best-in-class performance for a UTM firewall, these results suggest that testing using your own traffic mix is an important part of any performance-critical deployment.

SONICWALL®

1143 Borregas Avenue
Sunnyvale, CA 94089
888.557.6642
www.sonicwall.com