NETWORKWORLD Reprint

THE CONNECTED ENTERPRISE ≡ APRIL 23, 2012

CLEAR CHOICE TEST: NEXT-GENERATION FIREWALLS (PART 1)

Fast-forwarding firewall faceoff

SonicWall comes out on top in performance tests, but trade-offs remain

BY DAVID NEWMAN

Next-generation firewalls claim to identify application-layer attacks and enforce application-specific policies while delivering top-notch performance, even with advanced security features turned on.

In the first installment of this two-part Clear Choice test, we tackle the performance issue, evaluating NGFWs from Barracuda, Check Point, Fortinet, and SonicWall (recently acquired by Dell). On May 7, we'll present Joel Snyder's analysis of the features and functionality of these same devices.

Our overall conclusion is that next-gen firewalls are getting faster, and the trade-off between speed and security is definitely getting smaller, but it's still there.

While all devices moved traffic at multigigabit rates while doing application inspection, forwarding rates fell when we offered SSL traffic, and plummeted when we turned on SSL decryption.

In our tests, SonicWall's SuperMassive, the most expensive of the four products, moved traffic the fastest, even when forwarding SSL traffic. In multiple cases it maxed out the capabilities of our test bed. For example, when doing application inspection of cleartext traffic, it moved traffic at or near 20Gbps. That's even faster than Palo Alto's PA-5060, which hit 17Gbps in a test we conducted last year.

Fortinet's FortiGate 3950B also pushed the limits of our test bed and finished a close second to Sonic-Wall in tests involving cleartext traffic. It also handled slightly more TCP connections than the SonicWall device.

There was no performance slowdown with either the SonicWall or Fortinet devices when IPS and unified threat management (UTM) were turned on. Conversely, turning on IPS and UTM in the Barracuda and Check Point systems carried a heavy performance cost.

Check Point ran away with our toughest test. The Check Point 12610 proved by far the fastest at SSL decryption across all device configurations and was the only system to break the 1Gbps barrier (the SonicWall device ran faster, but only when we changed our test configuration to offer more flows).

Barracuda, the lowest-cost device in our test, delivered a solid 12Gbps when we measured cleartext throughput using mixed content types.

Mixed-content loads

We measured forwarding rates for mixed and static-length HTTP and SSL content; rates with SSL decryption enabled; and TCP scalability. We put the greatest emphasis on the mixed HTTP tests, because they most closely approximate the loads handled by firewalls in enterprise networks.

A key goal was to compare results with those of the Palo Alto PA-5060, which we evaluated in 2011 using the same methodology.

The mixed-content tests involved a variety of object sizes, like enterprise traffic, ranging from 1KB to 1.536MB, and a variety of content types, including .jpeg images, PDF documents, binary files and text objects.

We set up the Spirent Avalanche traffic generator to offer this mixed-content load to each NGFW in three different modes: as a firewall only; as a firewall and IPS; and as a UTM device with all functions enabled (firewall, IPS, antispyware, and antivirus [anti-bot in Check Point's case]). For all three modes, we offered both cleartext Web and SSL traffic. We also ran separate tests involving decrypted SSL traffic, to be discussed later.

These NGFWs always had application inspection enabled. The ability to classify traffic and make forwarding decisions at the application layer is what distinguishes NGFWs from previous-generation firewalls, IPSs and other security devices.

NGFWs generally run fastest when they function as straight firewalls handling unencrypted traffic (see graphic below). In terms of combined forwarding rate (adding incoming and outgoing traffic rates), SonicWall's SuperMassive was fastest, followed closely by Fortinet's FortiGate 3950B. Both products moved cleartext traffic at or near 20Gbps, the highest rate possible in one direction on our

NETRESULTS

Product	NG Firewall F900	Check Point 12610	FortiGate 3950B	SuperMassive E10800
Company	Barracuda Networks	Check Point Software	Fortinet	SonicWall
Cost	Base unit, $32,999; 8-port Gigabit copper module, $1,649; 2-port 10G Ethernet SFP+ module, $4,699	12610 appliance, $65,000; management appliance, $25,000	Base unit, $79,995; additional 2-port 10G module, $23,995	Base unit, $198,000; with IPS, anti-malware and application control, $261,400
Pros	Application inspection at up to 12Gbps	Highest SSL decryption rates	High transfer rates for Web traffic; highest TCP connection capacity	Fastest performer overall; highly scalable as user count grows
Cons	High cost to enabling IPS and UTM; lower TCP scalability than others	UTM features exact a performance cost	Significantly slower with SSL traffic	Most expensive system tested

test bed. (All systems had four 10G Ethernet interfaces, with servers on one side and clients on the other.)

Both the SonicWall and Fortinet devices came close to maxing out the test bed's network capacity not only in the firewall-only tests but also when configured with IPS and antivirus/anti-spyware features enabled.

These numbers also compare favorably with the ones posted last year by Palo Alto's PA-5060, which topped out at around 17Gbps as a firewall, but fell to 5.3Gbps in IPS mode and IPS plus UTM modes.

SSL rates were generally lower than those for cleartext traffic. This isn't surprising given that even without decryption, an application inspection engine may work harder to identify the seemingly random patterns in an SSL stream.

However, there were some exceptions: Check Point's 12610 moved SSL traffic faster than straight HTTP, and in one case so did Barracuda's NG Firewall F900. The most likely explanation is that once the devices identified traffic as SSL, they stopped any further attempts at traffic classification.

One configuration gotcha surprised at least two vendors' test engineers: When the Check Point and Fortinet systems had both SSL firewall rules and application inspection enabled, the inspection logic kicked in twice, causing SSL rates to be around half what each vendor expected to see.

The Check Point and Fortinet results were obtained without a specific SSL firewall rule, since the application inspection feature can identify SSL traffic and block or forward it as necessary. If this configuration issue can trip up firewall vendors' own engineers, it's definitely something for enterprise network managers to look out for.

Moving across the different configurations, the Barracuda firewall's forwarding rates dropped sharply when we enabled IPS and then all UTM features. Check Point's 12610 also moved cleartext traffic more slowly with antivirus and anti-bot features enabled; its SSL performance was about the same in all three configurations, again suggesting the device stopped inspection upon identifying a flow as SSL.

Static object tests

Tests of static 100KB and 512KB objects produced results similar to those involving mixed content. Devices generally moved static objects far faster over HTTP than SSL (see graphic below).

The Fortinet and SonicWall firewalls again moved cleartext HTTP objects at or near the network limits of our test. SonicWall's SuperMassive also came close to maxing out the SSL capabilities of our test bed. With no DUT in place, the Avalanche traffic generators moved 100KB and 512KB objects over SSL at 17.1Gbps and 14.4Gbps, respectively.

The SuperMassive moved SSL traffic near those rates, regardless of configuration. The performance degradation was more noticeable for Fortinet's FortiGate 3950B.

Also, as in the mixed-object tests, both the Fortinet and SonicWall devices moved traffic faster than Palo Alto's PA-5060 did in last year's tests. As a straight firewall, the PA-5060's top speed was 18.7Gbps with 512KB objects. That rate fell to 6.1Gbps in IPS mode and 6.3Gbps in UTM mode.

Conversely, the Barracuda and Check Point firewalls generally moved SSL traffic faster than plain HTTP, in one case — for Check Point — more than three times faster. Once again, both devices probably stopped inspecting traffic after classifying it as SSL.

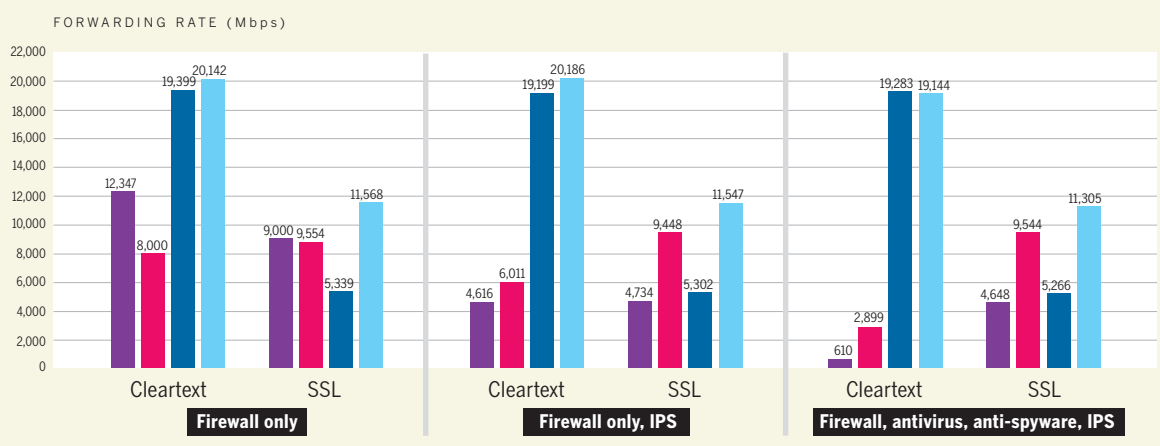
When IPS or UTM modes were turned on, both the Barracuda and Check Point firewalls slowed down, but the Fortinet and SonicWall devices moved traffic at roughly the same rate regardless of device configuration.

SSL decryption

SSL traffic poses a dual problem for NGFWs: If traffic is encrypted, applications cannot be inspected, but if traffic is decrypted there may be a very high performance cost. In fact, the SSL decryption tests turned out to be the biggest differentiator in this comparison, and for SonicWall the most controversial issue.

Mixed-HTTP Content Handling

The SonicWall and Fortinet devices maxed out the 20Gbps limit of our test bed with cleartext (unencrypted) Web traffic, but all devices moved SSL traffic at lower rates. And enabling IPS and UTM features caused further slowdowns for the Barracuda and Check Point devices when handling cleartext Web traffic.



When doing SSL decryption, a firewall acts as a proxy, intercepting client requests and replacing the server's certificate with its own. Since users seldom inspect the replaced "server" certificate, they think they're dealing directly with the origin server. The firewall, meanwhile, decrypts and inspects traffic contents.

Barracuda's current software works as a non-transparent proxy, requiring reconfiguration of all client browsers for decryption to work. Barracuda says a forthcoming software release will support transparent proxying. The other three devices all functioned as transparent proxies.

Also, the Barracuda and Fortinet devices only perform SSL decryption when antivirus inspection is enabled. The results given here reflect that; even though our methodology called for decryption in firewall-only and firewall-plus-UTM modes, the firewall-only numbers for Barracuda and Fortinet were obtained with antivirus inspection enabled.

Check Point's 12610 proved by far the fastest at SSL decryption across all device configurations. It also was the only system tested to break the 1Gbps barrier (see graphic , page 4).

Neither the Fortinet nor SonicWall devices decrypted SSL traffic at rates anywhere close to their rates without SSL decryption. Decryption rates for Fortinet's FortiGate 3950B ranged between 191Mbps and 472Mbps, far slower than its 3.6Gbps to 6.0Gbps range of rates without decryption.

Decryption rates fell even more precipitously for SonicWall's SuperMassive, but the vendor disputed our methodology. In our tests, the SuperMassive moved SSL traffic at 11.3Gbps without decryption, even with UTM features enabled; with decryption, the same load moved at just 83Mbps, slower than the 108Mbps low-water mark seen in the previous Palo Alto PA-5060 test. The rates were slower still, down to 49Mbps, with static 100KB objects, compared with 626Mbps for the PA-5060 in last year's test.

SonicWall says the SuperMassive can decrypt traffic at far higher rates, provided it's pushed harder. The vendor noted that its device's CPU utilization during these tests was only around 2%, suggesting it was capable of doing around 50 times more work.

To put that assertion to the test, we conducted one-off tests with 50 times more flows, and found that SuperMassive decrypted traffic at rates of up to 4.8Gbps (see "Scaling up with SonicWall's SuperMassive" at tinyurl.com/c4mem5b). We also tried the same large-flow-count tests with the other firewalls, but none could operate at this level without some failed transactions.

Even though the results show a big performance hit for all devices with SSL decryption, things actually could be much worse. We used the relatively weak RC4-MD5 cipher in these tests. While that's the cipher in use at many e-commerce sites, most banks and other financial institutions use much stronger ciphers, such as AES256-SHA1, that are far more compute-intensive and presumably would result in still lower forwarding rates.

TCP scalability

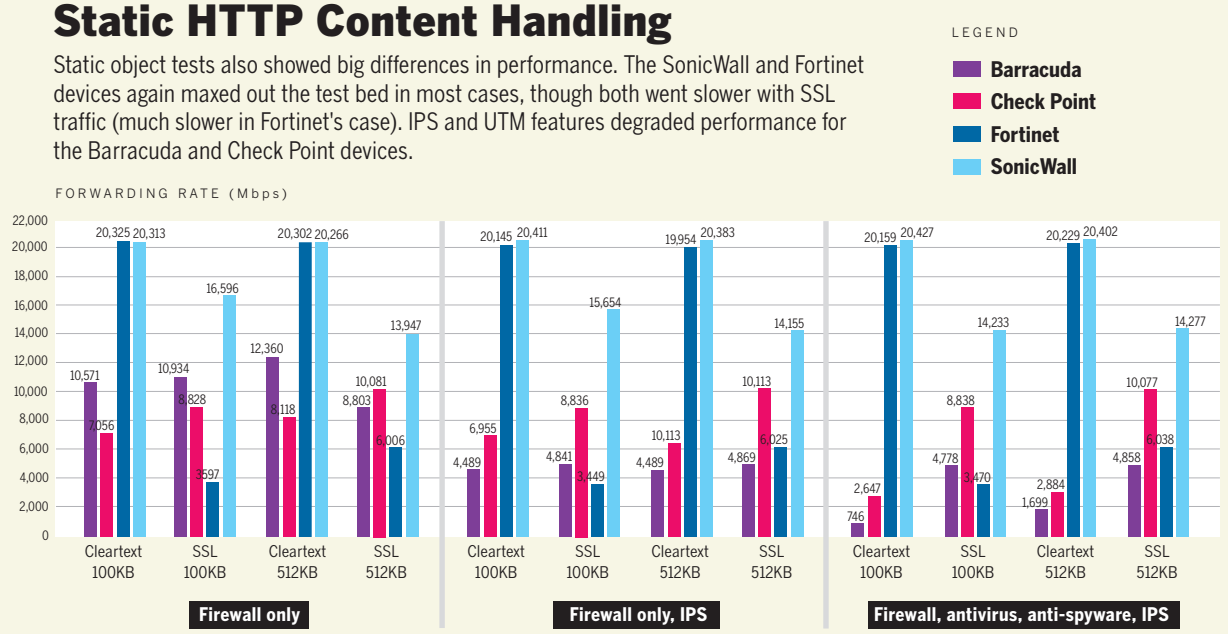
The final set of tests examined TCP scalability in two ways: in terms of capacity (the maximum number of concurrent connections each device could sustain without time-outs or other failures) and rate (the maximum speed at which each device could set up and tear down new connections, again with zero failures).

In the connection capacity tests, we configured Spirent Avalanche to build up successively larger connection counts by having each existing connection make one new HTTP request every 60 seconds. Fortinet's FortiGate 3950B took top honors here, handling more than 10 million connections. SonicWall's SuperMassive was close behind, successfully fielding 9.9 million connections. The Check Point and Barracuda systems handled far fewer concurrent connections, at 900,000 and 320,000, respectively.

To measure connection setup rate, we configured Spirent Avalanche to use the older HTTP 1.0 specification, which requires a new TCP connection for each new transaction. SonicWall's SuperMassive was the clear leader, setting up 290,000 connections per second (cps). Check Point's firewall was next, setting up 57,039 cps, while the Barracuda and Fortinet firewalls set up connections at 47,043 and 42,911 cps, respectively. The SuperMassive's

Static HTTP Content Handling

Static object tests also showed big differences in performance. The SonicWall and Fortinet devices again maxed out the test bed in most cases, though both went slower with SSL traffic (much slower in Fortinet's case). IPS and UTM features degraded performance for the Barracuda and Check Point devices.



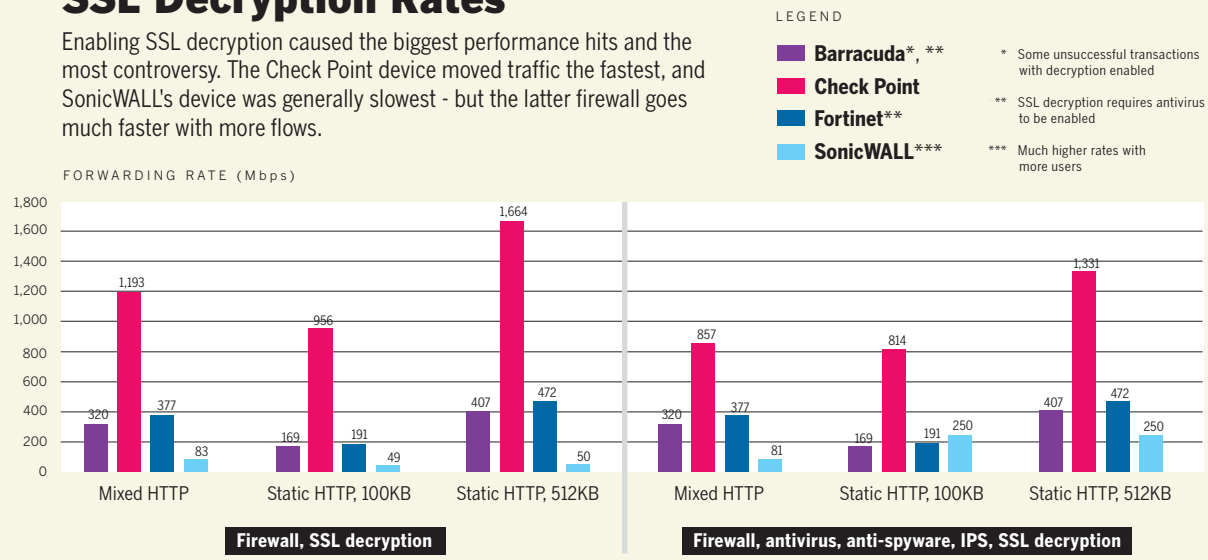
highly parallelized architecture (using 96 CPU cores) clearly favors a test like this.

We concluded last year's review of the Palo Alto PA-5060 saying there's room for improvement when it comes to NGFW performance. The vendors in this review have taken note: Forwarding rates are generally higher, as is TCP scalability. Further, some devices decrypt SSL traffic far faster than in previous tests. While there's still a security/performance trade-off — a big one — when decrypting SSL traffic, it's clear there are now more choices for high-speed application inspection and control. ■

Newman is a member of the Network World Lab Alliance and president of Network Test, an independent test lab and engineering services consultancy. He can be reached at dnewman@networktest.com.

SSL Decryption Rates

Enabling SSL decryption caused the biggest performance hits and the most controversy. The Check Point device moved traffic the fastest, and SonicWALL's device was generally slowest - but the latter firewall goes much faster with more flows.



Scaling Up With SonicWALL's Supermassive

BY DAVID NEWMAN

SonicWALL's initial response to results of our SSL decryption tests was "you've got to be kidding—we go way faster than that." Indeed, the vendor's internal tests showed the Supermassive decrypting SSL traffic at rates well into the gigabit range, compared with less than 100Mbps in some of our tests.

The difference has to do with the rate at which we offered traffic, and the results say something interesting about the way highly parallel systems work.

The Supermassive is aptly named. Its CPUs have 96 cores (and up to 384 cores in a high-availability cluster with four systems). As new flows come in, the system assigns them to new cores, repeating the process until all cores are fully utilized.

The forwarding-rate tests used the same configuration as the earlier evaluation of Palo Alto's PA-5060, with the Spirent Avalanche traffic generator configured to emulate concurrent 126 "SimUsers" (a load-generation concept similar to one user going through a list of URLs). With that load, the Supermassive's overall system CPU utilization barely topped 2%, suggesting it had plenty of headroom to handle higher traffic rates.

As SonicWALL predicted, rates shot up—way up—as we added SimUsers. The maximum load its system could handle without errors was around 5,800 SimUsers. The resulting forwarding rates - around 4.8Gbps in some cases—were far higher than those with 126 SimUsers.

We also tried a few SSL decryption tests with 5,800 SimUsers on the other vendors' systems, but none could handle that load without at least some transaction failures.

SonicWALL says the difference in results isn't so much a function of the number of users as the rate at which we offered traffic. We agree; on a per-user basis, the rates are pretty similar in the 126- and 5,800-SimUser tests. In this light, there's merit to SonicWALL's assertion that the 126-SimUser configuration didn't push its device hard enough.

On the other hand, other devices moved traffic from the same 126-SimUser configuration at higher rates. Since we used the same test with all devices, the different results can only be explained by device architecture. The other devices tested may have had higher CPU utilization, or deeper buffers, or both.

SonicWALL's Supermassive can decrypt SSL traffic very fast—in fact these one-off tests show it to be the fastest device by far. At the same time, its highly parallel architecture may produce lower rates in situations where a relatively few flows are active at any given time.

SONICWALL®

© Copyright 2012 by Network World, Inc., Southborough, MA 01772-9108 • Posted from *Network World.com* • Trademark is owned by International Data Group, Inc.
#C9229 Managed by The YGS Group, 800.290.5460. For more information visit www.theYGSgroup.com/content.