NEXT GENERATION FIREWALL COMPARATIVE REPORT

Total Cost of Ownership (TCO)

JUNE 06, 2017

Authors – Thomas Skybakmoen, Morgan Dhanraj

Tested Products

Barracuda NextGen Firewall F600.E20 Firmware Version 7.0.2

Check Point Software Technologies 15600 Next Generation Threat Prevention (NGTP) Appliance R77.20

Cisco Firepower 4110 v6.1.0.1

Forcepoint NGFW 3301 Appliance v6.1.2

Fortinet FortiGate 3200D FortiOS v5.4.4 GA Build 1117

Fortinet FortiGate 600D FortiOS v5.4.4 GA Build 1117

Juniper Networks SRX 4200 v15.1X49-D75.5

Palo Alto Networks PA-5250 PAN-OS 8.0.0

SonicWall NSA 6600 SonicOS 6.2

Sophos XG-750 Firewall v16.01

WatchGuard Firebox M4600 v11.10.7

Environment

Next Generation Firewall (NGFW) Test Methodology v7.0

Overview

The implementation of next generation firewall (NGFW) devices can be a complex process, with multiple factors affecting the overall cost of deployment, maintenance, and upkeep. Enterprises should include the total cost of ownership (TCO) as part of their evaluations, focusing on the following at a minimum:

- Acquisition costs for NGFW devices and a central management system (CMS)
- Fees paid to the vendor for annual maintenance, support, and signature updates
- Labor costs for installation, maintenance, and upkeep

NSS Labs invited NGFW vendors to submit their products for testing at no cost. Throughput of the submitted products ranged from approximately 2.6 Gbps to 24 Gbps, which accounts for differences in TCO. No two network security systems deliver the same security effectiveness or performance, making precise comparisons extremely difficult. In order to enable value-based comparisons of NGFW products on the market, NSS has developed a unique formula: *TCO per Protected Mbps*. Using this formula, NSS is able to normalize data and account for wide-ranging differences in TCO and performance among products. See Figure 1 for details.

Within a given performance range (*NSS-Tested Throughput*), the *TCO per Protected Mbps* metric provides clear guidance as to whether a product's price is higher or lower than the majority of its competitors. A high price could indicate a premium based on security effectiveness, brand recognition, or level of customer service. Conversely, a high price could also be a penalty for purchasing an underperforming product.

***Security Effectiveness* = Firewall** (Firewall Policy Enforcement * Application Control * **IPS** (Exploit Block Rate[1] * Evasions) * **Stability and Reliability**
TCO per Protected Mbps = TCO / (*Security Effectiveness* * NSS-Tested Throughput)

Figure 1 – Security Effectiveness and TCO per Protected Mbps Formulas

For the purposes of this analysis, NSS developed an enterprise use case with one CMS and five devices deployed across multiple remote locations.

Product	Purchase Price	Security Effectiveness	3-Year TCO	TCO per Protected Mbps
Barracuda Networks	$75,244	25.8%	$143,416	$39
Check Point	$230,525	89.6%	$449,360	$18
Cisco	$132,495	95.5%	$244,875	$21
Forcepoint	$225,545	99.9%	$386,833	$8
Fortinet 3200D	$301,700	78.6%	$683,105	$9
Fortinet 600D	$31,700	78.6%	$73,925	$5
Juniper Networks	$168,600	37.8%	$387,956	$105
Palo Alto Networks	$715,000	39.7%	$718,000	$20
SonicWall	$79,980	26.4%	$193,335	$39
Sophos	$110,885	90.4%	$226,220	$6
WatchGuard	$79,495	88.9%	$82,495	$8

Figure 2 – TCO per Protected Mbps Results for Tested Products (US$)

[1] Exploit block rate is defined as the number of live exploits (CAWS) and exploits from the *NSS Exploit Library* blocked under test. See the NGFW Comparative Report on Security for more detail.

Table of Contents

Table of Figures

Total Cost of Ownership

Tuning

NGFW products are complex. With a shortage of skilled and experienced security professionals, enterprises should consider the time and resources required to properly install and maintain the solution. Failure to do so could result in products not achieving their full security potential.

NSS research indicates that NGFW devices are typically deployed to protect users rather than data center assets, and that the majority of enterprises will not separately tune intrusion prevention system (IPS) modules within their NGFWs. Therefore, during NSS testing, NGFW products are configured with the vendor's pre-defined or recommended (i.e., "out-of-the-box") settings in order to provide readers with relevant *Security Effectiveness* and performance metrics based on their expected usage.

Figure 3 depicts the labor required to take the device out of the box, configure it, deploy it in the network, apply updates and patches, perform initial tuning, and set up desired logging and reporting.

Labor for Device Setup

Costs are based on the time that would be required by an experienced security engineer to perform the setup tasks listed above. The calculations assume a rate of US$75 per hour. Clients can use the Security Value Map™ (SVM) Toolkit and substitute their own costs to get accurate TCO figures.

Product	Installation (Hours)
Barracuda Networks	8
Check Point	8
Cisco	8
Forcepoint	8
Fortinet 3200D	8
Fortinet 600D	8
Juniper Networks	8
Palo Alto Networks	8
SonicWall	8
Sophos	8
WatchGuard	8

Figure 3 – Labor per NGFW Device (Hours)

Labor for Central Management

Enterprises should include labor costs for operational expenditures (opex) when evaluating NGFW devices. These costs would include day-to-day management tasks such as administration, policy and configuration handling, log handling, alert handling, monitoring, reporting, analysis, auditing and compliance, maintenance, software updates, and troubleshooting.

NSS does not include opex in this analysis. NSS clients can model these costs using the SVM Toolkit or they can schedule an inquiry call with NSS analysts.

Equipment and Software Costs

All capital expenditure (capex) costs are based on list prices provided by vendors at the time of the test. The actual cost to end users may be lower depending on the negotiated discount. However, it is fair to assume that all vendors will provide a similar discount, resulting in a relatively constant cost ratio. Costs are depicted in Figure 4.

	Initial Purchase		Annual Cost	
Product	Device as Tested	Price (CMS)	Maintenance and Support (Hardware/Software)	Maintenance and Support (CMS)
Barracuda Networks	$14,249	$3,999	$4,225	$599
Check Point	$44,605	$7,500	$13,954	$2,175
Cisco	$26,099	$2,000	$7,200	$460
Forcepoint	$45,109	$0	$10,150	$2,013
Fortinet 3200D	$60,000	$1,700	$25,125	$510
Fortinet 600D	$6,000	$1,700	$2,513	$510
Juniper Networks	$33,000	$3,600	$14,316	$539
Palo Alto Networks	$140,000	$15,000	$0	$0
SonicWall	$15,996	$0	$7,198	$795
Sophos	$22,177	$0	$7,489	$0
WatchGuard	$15,899	$0	$0	$0

Figure 4 – Equipment and Software Costs (US$)[2]

NSS clients can use the SVM Toolkit to model actual negotiated prices, labor costs, and upkeep times.

[2] Pricing has been normalized in some cases for CMS costs. For more information, please contact NSS Labs.

TCO Calculations

The TCO incorporates capex over a three-year period, including initial acquisition and deployment costs and annual maintenance and update costs (software and hardware updates). Calculations are as follows:

Value	Description of Calculation
Year 1 Cost	Initial Purchase Price + Maintenance Cost + (Installation x Labor rate $/hr)
Year 2 Cost	Maintenance Cost
Year 3 Cost	Maintenance Cost
3-Year TCO	Year 1 Cost + Year 2 Cost + Year 3 Cost

Figure 5 – TCO Calculations

Calculations are based on a labor rate of US$75 per hour and vendor-provided pricing information. Where possible, the 24/7 maintenance and support option with 24-hour replacement is used, since enterprise customers typically select that option. Pricing includes one enterprise-class CMS to manage up to five devices.

Product	Purchase Price	Maintenance per Year	Year 1 Product Cost	Year 1 Labor Cost	1-Year TCO
Barracuda Networks	$75,244	$21,724	$96,968	$3,000	$99,968
Check Point	$230,525	$71,945	$302,470	$3,000	$305,470
Cisco	$132,495	$36,460	$168,955	$3,000	$171,955
Forcepoint	$225,545	$52,763	$278,308	$3,000	$281,308
Fortinet 3200D	$301,700	$126,135	$427,835	$3,000	$430,835
Fortinet 600D	$31,700	$13,075	$44,775	$3,000	$47,775
Juniper Networks	$168,600	$72,119	$240,719	$3,000	$243,719
Palo Alto Networks	$715,000	$0	$715,000	$3,000	$718,000
SonicWall	$79,980	$36,785	$116,765	$3,000	$119,765
Sophos	$110,885	$37,445	$148,330	$3,000	$151,330
WatchGuard	$79,495	$0	$79,495	$3,000	$82,495

Figure 6 –1-Year TCO (US$)

Note that opex is excluded from TCO calculations for the purposes of this report, but NSS clients can model these costs using the SVM Toolkit.

Normalizing TCO Data

The benefit of normalization is that, within a given performance range (*NSS-Tested Throughput*), the *TCO per Protected Mbps* metric provides clear guidance as to whether a product's price is higher or lower than the majority of its competitors. A high price could indicate a premium based on security effectiveness, brand recognition, or level of customer service. Conversely, a high price could also be a penalty for purchasing an underperforming product.

There are multiple methods by which *Value* can be determined:

Purchase Price Based on Vendor-Claimed Throughput

The simplest means of determining *Value*, but also the most misleading, is to determine the purchase price per Mbps based on the vendor-claimed throughput and the initial purchase price of the product.

TCO Based on Vendor-Claimed Throughput

A more accurate calculation would be to determine the TCO per vendor-claimed throughput (in the case of NGFW, this would be Mbps). This calculation is performed in many purchasing departments. Unfortunately, this approach is as flawed as the first approach, since it relies on the vendor-claimed throughput without performing independent tests to determine the *actual* throughput of the device under real-world conditions.

TCO Based on NSS-Tested Throughput

Vendor throughput claims are frequently exaggerated in marketing materials, or they simply fail to take into account real-world deployment conditions. Knowing this, many enterprise IT professionals will over-purchase based on throughput to ensure adequate performance headroom. *NSS-Tested Throughput* is a real-world representation of a product's performance. *NSS-Tested Throughput* is often significantly different from vendor-claimed throughput (see Figure 7). For more information on *NSS-Tested Throughput*, see the Comparative Report on Performance at www.nsslabs.com.

Product	Vendor-Claimed Throughput (Mbps)	NSS-Tested Throughput (Mbps)	% Delta
Barracuda Networks	2,600	2,842	9%
Check Point	5,200	5,516	6%
Cisco	10,000	2,495	-75%
Forcepoint	9,000	9,952	11%
Fortinet 3200D	24,000	18,573	-23%
Fortinet 600D	3,200	3,688	15%
Juniper Networks	15,000	1,955	-87%
Palo Alto Networks	20,300	17,740	-13%
SonicWall	3,000	3,772	26%
Sophos	11,800	8,628	-27%
WatchGuard	3,000	2,472	-18%

Figure 7 – Vendor-Claimed Throughput vs. NSS-Tested Throughput

TCO Based on Security Effectiveness

Determining value solely based on TCO and throughput is acceptable when dealing with a pure networking device. However, for security devices, *Security Effectiveness* must also be factored into the equation. The *Security Effectiveness* of a device factors in block rate, evasions, and stability and reliability scores (see Figure 1). Each of these factors can have a serious impact on *Security Effectiveness*. NSS is aware of these limitations and has developed a unique metric termed *TCO per Protected Mbps* to enable value-based comparisons of NGFW products on the market. See Figure 1 for details.

Figure 8 depicts the calculation for *TCO per Protected Mbps*, which is based on the product's three-year TCO and *Security Effectiveness* ratings. For more information on the calculations, schedule an inquiry call with NSS analysts or refer to the SVM Toolkit.

Product	Security Effectiveness	3-Year TCO	TCO per Protected Mbps
Barracuda Networks	25.8%	$143,416	$39
Check Point	89.6%	$449,360	$18
Cisco	95.5%	$244,875	$21
Forcepoint	99.9%	$386,833	$8
Fortinet 3200D	78.6%	$683,105	$9
Fortinet 600D	78.6%	$73,925	$5
Juniper Networks	37.8%	$387,956	$105
Palo Alto Networks	39.7%	$718,000	$20
SonicWall	26.4%	$193,335	$39
Sophos	90.4%	$226,220	$6
WatchGuard	88.9%	$82,495	$8

Figure 8 – TCO per Protected Mbps (US$)

Security Effectiveness and Value

Value is a metric that is distinct from both purchase price and TCO. Figure 9 and Figure 10 demonstrate the ways in which the actual value of a product can change significantly as *NSS-Tested Throughput* and *Security Effectiveness* are factored in. In Figure 9, reading from left to right, the value changes as additional test metrics are introduced. The value in the final column incorporates the three-year TCO, *NSS-Tested Throughput*, and *Security Effectiveness* as determined by NSS testing.

Product	Vendor-Claimed Throughput (Mbps) TCO per Mbps	Vendor-Claimed Throughput (Mbps) + Exploit Block Rate TCO per Protected Mbps	NSS-Tested Throughput (Mbps) + Exploit Block Rate TCO per Protected Mbps	NSS-Tested Throughput (Mbps) + Security Effectiveness TCO per Protected Mbps
Barracuda Networks	$11	$12	$11	$39
Check Point	$17	$17	$16	$18
Cisco	$5	$5	$21	$21
Forcepoint	$9	$9	$8	$8
Fortinet 3200D	$6	$6	$7	$9
Fortinet 600D	$5	$5	$4	$5
Juniper Networks	$5	$5	$41	$105
Palo Alto Networks	$7	$7	$8	$20
SonicWall	$13	$13	$10	$39
Sophos	$4	$4	$5	$6
WatchGuard	$5	$6	$7	$8

Figure 9 – Value Based on TCO per Protected Mbps (US$)

Figure 10 compares the vendor-claimed *Value* metric with the metric generated from NSS test results. The *Security Effectiveness* value indicates whether a product is underpriced, overpriced, or priced accurately depending on the *NSS-Tested Throughput* and overall *Security Effectiveness*.

A product with a *Security Effectiveness* value that is higher than its purchase price can be considered to have a good value. A product with a purchase price that is higher than its *Security Effectiveness* value can be considered overpriced.

Product	Purchase Price	Security Effectiveness Value	Delta	% Delta
Barracuda Networks	$75,244	$34,224	($41,020)	-55%
Check Point	$230,525	$230,525	$0	0%
Cisco	$132,495	$111,105	($21,390)	-16%
Forcepoint	$225,545	$463,898	$238,353	106%
Fortinet 3200D	$301,700	$680,713	$379,013	126%
Fortinet 600D	$31,700	$135,175	$103,475	326%
Juniper Networks	$168,600	$34,505	($134,095)	-80%
Palo Alto Networks	$715,000	$328,836	($386,164)	-54%
SonicWall	$79,980	$46,516	($33,464)	-42%
Sophos	$110,885	$363,854	$252,969	228%
WatchGuard	$79,495	$102,475	$22,980	29%

Figure 10 – Purchase Price vs. Security Effectiveness Value

Test Methodology

Next Generation Firewall Test Methodology v7.0

A copy of the test methodology is available on the NSS Labs website at www.nsslabs.com.

Contact Information

NSS Labs, Inc.
206 Wild Basin Road
Building A, Suite 200
Austin, TX 78746
info@nsslabs.com
www.nsslabs.com