



NEXT GENERATION FIREWALL COMPARATIVE REPORT

Total Cost of Ownership (TCO)

JULY 17, 2018

Author – Thomas Skybakmoen

Tested Products

Barracuda Networks CloudGen Firewall F800.CCE v7.2.0

Check Point 15600 Next Generation Threat Prevention (NGTP) Appliance vR80.20

Cisco Firepower 4120 Security Appliance v6.2.2

Forcepoint NGFW 2105 Appliance v6.3.3 build 19153 (Update Package: 1056)

Fortinet FortiGate 500E V5.6.3GA build 7858

Palo Alto Networks PA-5220 PAN-OS 8.1.1

SonicWall NSa 2650 SonicOS Enhanced 6.5.0.10-73n

Sophos XG Firewall 750 SFOS v17 MR7

Versa Networks FlexVNF 16.1R1-S6

WatchGuard M670 v12.0.1.B562953

Environment

NSS Labs Next Generation Firewall Test Methodology v8.0

NSS Labs SSL/TLS Performance Test Methodology v1.3

NSS Labs Evasions Test Methodology v1.1

Overview

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 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 2.4 Gbps to 20 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.

$$\begin{aligned}
 \text{Security Effectiveness} &= \text{Exploit Block Rate}^1 * \text{Evasions} * \text{Stability and Reliability} \\
 \text{TCO per Protected Mbps} &= \text{TCO} / (\text{Security Effectiveness} * \text{NSS-Tested Throughput})
 \end{aligned}$$

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.

Vendor	Purchase Price	Security Effectiveness	3-Year TCO	TCO per Protected Mbps
Barracuda Networks	\$105,704	95.4%	\$196,022	\$8
Check Point	\$221,375	25.0%	\$399,433	\$57
Cisco	\$285,685	71.8%	\$535,909	\$28
Forcepoint	\$145,395	99.7%	\$240,533	\$6
Fortinet	\$27,950	99.3%	\$59,858	\$2
Palo Alto Networks	\$195,000	98.7%	\$270,000	\$7
SonicWall	\$14,370	98.8%	\$22,359	\$4
Sophos	\$78,270	25.0%	\$160,560	\$22
Versa Networks	\$59,475	90.4%	\$63,225	\$4
WatchGuard	\$18,560	89.1%	\$58,680	\$8

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

¹ Exploit block rate is defined as the total number of samples (live exploits and exploits from the NSS Labs Exploit Library) that are blocked under test. See the NGFW Comparative Report on Security for more detail.

Table of Contents

Tested Products	1
Environment	1
Overview	2
Total Cost of Ownership	4
Tuning.....	4
Labor for Device Setup.....	4
Labor for Central Management	5
Equipment and Software Costs	5
TCO Calculations	6
Normalizing TCO Data	6
Purchase Price Based on Vendor-Claimed Throughput.....	7
TCO Based on Vendor-Claimed Throughput.....	7
TCO Based on NSS-Tested Throughput	7
TCO Based on Security Effectiveness	8
Security Effectiveness and Value	9
Test Methodology	11
Contact Information	11

Table of Figures

Figure 1 – Security Effectiveness and TCO per Protected Mbps Formulas.....	2
Figure 2 – TCO per Protected Mbps Results for Tested Products (US\$).....	2
Figure 3 – Labor per NGFW Device (Hours).....	4
Figure 4 – Equipment and Software Costs (US\$).....	5
Figure 5 – TCO Calculations	6
Figure 6 –1-Year TCO (US\$).....	6
Figure 7 – Vendor-Claimed Throughput vs. NSS-Tested Throughput.....	7
Figure 8 – TCO per Protected Mbps (US\$).....	8
Figure 9 – Value Based on TCO per Protected Mbps (US\$)	9
Figure 10 – Purchase Price vs. Security Effectiveness Value	10

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 device. 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.

Vendor	Installation (Hours)
Barracuda Networks	8
Check Point	8
Cisco	8
Forcepoint	8
Fortinet	8
Palo Alto Networks	8
SonicWall	8
Sophos	8
Versa Networks	10
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.

Vendor	Initial Purchase		Annual Cost	
	Device as Tested	Price (CMS)	Maintenance and Support (Hardware/Software)	Maintenance and Support (CMS)
Barracuda Networks	\$20,049	\$5,459	\$5,670	\$756
Check Point	\$43,450	\$4,125	\$11,420	\$1,251
Cisco	\$56,997	\$700	\$16,448	\$168
Forcepoint	\$29,079	\$0	\$5,740	\$2,013
Fortinet	\$5,250	\$1,700	\$1,838	\$446
Palo Alto Networks	\$37,500	\$7,500	\$4,800	\$0
SonicWall	\$2,495	\$1,895	\$300	\$163
Sophos	\$15,654	\$0	\$5,286	\$0
Versa Networks	\$11,895	\$0	\$0	\$0
WatchGuard	\$3,712	\$0	\$2,475	\$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.

Vendor	Purchase Price	Maintenance per Year	Year 1 Product Cost	Year 1 Labor Cost	1-Year TCO
Barracuda Networks	\$105,704	\$28,350	\$134,054	\$3,000	\$137,810
Check Point	\$221,375	\$57,102	\$278,477	\$3,000	\$282,728
Cisco	\$285,685	\$82,240	\$367,925	\$3,000	\$371,093
Forcepoint	\$145,395	\$28,700	\$174,095	\$3,000	\$179,108
Fortinet	\$27,950	\$9,190	\$37,140	\$3,000	\$40,586
Palo Alto Networks	\$195,000	\$24,000	\$219,000	\$3,000	\$222,000
SonicWall	\$14,370	\$1,500	\$15,870	\$3,000	\$19,033
Sophos	\$78,270	\$26,430	\$104,700	\$3,000	\$107,700
Versa Networks	\$59,475	\$0	\$59,475	\$3,750	\$63,225
WatchGuard	\$18,560	\$12,373	\$30,933	\$3,000	\$33,933

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 an NGFW, this would be Mbps). This calculation is performed in many purchasing departments. Unfortunately, this is as flawed as the first approach, since it relies on 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.

Vendor	Vendor-Claimed Throughput (Mbps)	NSS-Tested Throughput (Mbps)	% Delta
Barracuda Networks	7,700	5,037	-35%
Check Point	5,200	5,599	8%
Cisco	15,000	5,291	-65%
Forcepoint	7,500	7,654	2%
Fortinet	5,200	6,753	30%
Palo Alto Networks	9,000	7,888	-12%
SonicWall	1,400	1,028	-27%
Sophos	11,800	5,844	-50%
Versa Networks	20,000	3,661	-82%
WatchGuard	2,400	1,589	-34%

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, *NSS-Tested Throughput (Mbps)*, and *Security Effectiveness* ratings. For more information on the calculations, schedule an inquiry call with NSS analysts or refer to the SVM Toolkit.

Vendor	Purchase Price	Security Effectiveness	3-Year TCO	TCO per Protected Mbps
Barracuda Networks	\$105,704	95.4%	\$196,022	\$8
Check Point	\$221,375	25.0%	\$399,433	\$57
Cisco	\$285,685	71.8%	\$535,909	\$28
Forcepoint	\$145,395	99.7%	\$240,533	\$6
Fortinet	\$27,950	99.3%	\$59,858	\$2
Palo Alto Networks	\$195,000	98.7%	\$270,000	\$7
SonicWall	\$14,370	98.8%	\$22,359	\$4
Sophos	\$78,270	25.0%	\$160,560	\$22
Versa Networks	\$59,475	90.4%	\$63,225	\$4
WatchGuard	\$18,560	89.1%	\$58,680	\$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 a product's actual value can change as *NSS-Tested Throughput* and *Security Effectiveness* are factored in. In Figure 9, reading from left to right, the value changes as 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.

	Vendor-Claimed Throughput (Mbps)	Vendor-Claimed Throughput (Mbps) + Exploit Block Rate	NSS-Tested Throughput (Mbps) + Exploit Block Rate	NSS-Tested Throughput (Mbps) + Security Effectiveness
Vendor	TCO per Mbps	TCO per Protected Mbps	TCO per Protected Mbps	TCO per Protected Mbps
Barracuda Networks	\$5	\$5	\$8	\$8
Check Point	\$15	\$15	\$14	\$57
Cisco	\$7	\$7	\$21	\$28
Forcepoint	\$6	\$6	\$6	\$6
Fortinet	\$2	\$2	\$2	\$2
Palo Alto Networks	\$6	\$6	\$7	\$7
SonicWall	\$3	\$3	\$4	\$4
Sophos	\$3	\$3	\$6	\$22
Versa Networks	\$1	\$1	\$4	\$4
WatchGuard	\$5	\$5	\$8	\$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.

Vendor	Purchase Price	Security Effectiveness Value	Delta	% Delta
Barracuda Networks	\$105,704	\$98,629	(\$7,075)	-7%
Check Point	\$221,375	\$28,732	(\$192,643)	-87%
Cisco	\$285,685	\$77,955	(\$207,730)	-73%
Forcepoint	\$145,395	\$156,631	\$11,236	8%
Fortinet	\$27,950	\$137,652	\$109,702	392%
Palo Alto Networks	\$195,000	\$159,871	(\$35,129)	-18%
SonicWall	\$14,370	\$20,848	\$6,478	45%
Sophos	\$78,270	\$29,992	(\$48,278)	-62%
Versa Networks	\$59,475	\$67,903	\$8,428	14%
WatchGuard	\$18,560	\$29,064	\$10,504	57%

Figure 10 – Purchase Price vs. Security Effectiveness Value

Test Methodology

NSS Labs Next Generation Firewall (NGFW) Test Methodology v8.0

NSS Labs SSL/TLS Performance Test Methodology v1.3

NSS Labs Evasions Test Methodology v1.1

Contact Information

3711 South Mopac Expressway

Building 1, Suite 400

Austin, TX 78746

info@nsslabs.com

www.nsslabs.com

This and other related documents are available at: www.nsslabs.com. To receive a licensed copy or report misuse, please contact NSS Labs.

© 2018 NSS Labs, Inc. All rights reserved. No part of this publication may be reproduced, copied/scanned, stored on a retrieval system, e-mailed or otherwise disseminated or transmitted without the express written consent of NSS Labs, Inc. (“us” or “we”).

Please read the disclaimer in this box because it contains important information that binds you. If you do not agree to these conditions, you should not read the rest of this report but should instead return the report immediately to us. “You” or “your” means the person who accesses this report and any entity on whose behalf he/she has obtained this report.

1. The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.
2. The information in this report is believed by us to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.
3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.
5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.
6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.