NEXT GENERATION INTRUSION PREVENTION SYSTEM (NGIPS) COMPARATIVE REPORT

Total Cost of Ownership (TCO)

OCTOBER 13, 2016

Authors – Thomas Skybakmoen, Chris Conrad, Tim Otto, Morgan Dhanraj

Tested Products

Check Point Software Technologies, Ltd. 13800 Next Generation Firewall Appliance vR77.20

Cisco FirePOWER 8350 v6.0.1

Forcepoint Stonesoft Next Generation Firewall 3301 v6.0.2

Fortinet FortiGate 3000D v5.4.0

IBM Security Network Protection XGS 7100 v5.3.2.1

Intel Security McAfee Network Security Platform NS9100 v8.2.5.158

Palo Alto Networks PA-7050 v7.0.4

Trend Micro TippingPoint 7500NX v3.8.4.4525

Environment

Next Generation Intrusion Prevention System Test Methodology v2.0

Overview

The implementation of next generation intrusion prevention system (NGIPS) products 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 the NGIPS devices and 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 all NGIPS vendors to submit their products for testing at no cost. Throughput for the submitted products ranged from around 10 Gbps to 60 Gbps, which would account 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 NGIPS 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 = 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 purpose of this analysis, NSS developed an enterprise use case with one CMS and four devices deployed across multiple remote locations.

Product	NSS-Tested Throughput (Mbps)	3-Year TCO (four devices + CMS)	Security Effectiveness	TCO per Protected Mbps
Check Point 13800	12,345	$396,241	99.9%	$8
Cisco FirePOWER 8350	21,713	$721,963	98.7%	$8
Forcepoint Stonesoft 3301	10,110	$404,226	99.6%	$10
Fortinet FortiGate 3000D	25,386	$438,830	24.9%	$17
IBM XGS 7100	21,886	$1,581,711	94.4%	$19
Intel Security McAfee NS9100	11,023	$926,984	98.5%	$21
Palo Alto Networks PA-7050	37,238	$4,033,480	99.3%	$27
Trend Micro TippingPoint 7500NX	12,856	$748,912	99.5%	$15

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

[1] Exploit block rate is defined as the number of exploits and live (real-time) drive-by exploits blocked under test.

Table of Contents

Table of Figures

Total Cost of Ownership

Tuning

NGIPS products are deployed at the perimeter and within corporate networks to protect employee desktops, laptops, and PCs. NSS research has determined that the majority of enterprises do not tune their NGIPS products, but rather rely on a vendor's default/recommended policies and settings. Since there are enterprises that do tune their devices, NSS has tested NGIPS products using both tuned and vendor-recommended settings.

NSS defines a Vendor-Recommended policy as an out-of-the-box, vendor-pre-defined policy that is available to all customers. NSS defines tuning as the act of changing the device setting from the default/recommended setting to a specific configuration based on the environment it is protecting. In both cases, the signatures/filters/rules that trigger false positives are turned off, since that is what would happen in an enterprise environment.

In order for enterprises to compare how policy changes impact security effectiveness, the product was tested using both recommended and tuned policies. Please see individual Test Reports for more detail.

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)
Check Point 13800	8
Cisco FirePOWER 8350	8
Forcepoint Stonesoft 3301	8
Fortinet FortiGate 3000D	8
IBM XGS 7100	8
Intel Security McAfee NS9100	8
Palo Alto Networks PA-7050	8
Trend Micro TippingPoint 7500NX	8

Figure 3 – Labor Cost per NGIPS (Hours)

Labor for Central Management

Enterprises should include labor costs for operational expenditures (opex) when evaluating an NGIPS. 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)
Check Point 13800	$56,155	$6,900	$10,051	$2,023
Cisco FirePOWER 8350	$120,905	$7,499	$18,686	$1,402
Forcepoint Stonesoft 3301	$39,310	$1,583	$12,091	$237
Fortinet FortiGate 3000D	$48,000	$1,700	$10,500	$510
IBM XGS 7100	$234,605	$3,980	$52,877	$796
Intel Security McAfee NS9100	$143,257	$5,995	$28,497	$1,199
Palo Alto Networks PA-7050	$820,000	$13,800	$23,040	$0
Trend Micro TippingPoint 7500NX	$111,998	$9,995	$23,519	$2,099

Figure 4 – Equipment and Software Costs (US$)

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

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 four devices.

Product	Purchase Price	Maintenance per Year	Year 1 Product	Year 1 Labor Cost	1-Year TCO
Check Point 13800	$231,520	$54,107	$285,627	$2,400	$288,027
Cisco FirePOWER 8350	$491,121	$76,148	$567,268	$2,400	$569,668
Forcepoint Stonesoft 3301	$158,821	$81,002	$239,823	$2,400	$242,223
Fortinet FortiGate 3000D	$193,700	$80,910	$274,610	$2,400	$277,010
IBM XGS 7100	$942,400	$212,304	$1,154,704	$2,400	$1,157,104
Intel Security McAfee NS9100	$579,023	$115,187	$694,210	$2,400	$696,610
Palo Alto Networks PA-7050	$3,293,800	$245,760	$3,539,560	$2,400	$3,541,960
Trend Micro TippingPoint 7500NX	$457,987	$96,175	$554,162	$2,400	$556,562

Figure 6 – Year 1 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 NGIPS, 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
Check Point 13800	6,400	12,345	93%
Cisco FirePOWER 8350	15,000	21,713	45%
Forcepoint Stonesoft 3301	8,000	10,110	26%
Fortinet FortiGate 3000D	25,000	25,386	2%
IBM XGS 7100	25,000	21,886	-12%
Intel Security McAfee NS9100	10,000	11,023	10%
Palo Alto Networks PA-7050	60,000	37,238	-38%
Trend Micro TippingPoint 7500NX	20,000	12,856	-36%

Figure 7 – Vendor-Claimed 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 NGIPS 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	NSS-Tested Throughput (Mbps)	3-Year TCO (four devices + CMS)	Security Effectiveness	TCO per Protected Mbps
Check Point 13800	12,345	$396,241	99.9%	$8
Cisco FirePOWER 8350	21,713	$721,963	98.7%	$8
Forcepoint Stonesoft 3301	10,110	$404,226	99.6%	$10
Fortinet FortiGate 3000D	25,386	$438,830	24.9%	$17
IBM XGS 7100	21,886	$1,581,711	94.4%	$19
Intel Security McAfee NS9100	11,023	$926,984	98.5%	$21
Palo Alto Networks PA-7050	37,238	$4,033,480	99.3%	$27
Trend Micro TippingPoint 7500NX	12,856	$748,912	99.5%	$15

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, the *NSS-Tested Throughput*, and *Security Effectiveness* as determined by NSS testing.

	Vendor-Claimed Throughput (Mbps)		NSS-Tested Throughput (Mbps)	
		Exploit Block Rate	Exploit Block Rate	Security Effectiveness
Product	TCO per Mbps	TCO per Protected Mbps	TCO per Protected Mbps	TCO per Protected Mbps
Check Point 13800	$15	$16	$8	$8
Cisco FirePOWER 8350	$12	$12	$8	$8
Forcepoint Stonesoft 3301	$13	$13	$10	$10
Fortinet FortiGate 3000D	$4	$4	$4	$17
IBM XGS 7100	$16	$17	$19	$19
Intel Security McAfee NS9100	$23	$24	$21	$21
Palo Alto Networks PA-7050	$17	$17	$27	$27
Trend Micro TippingPoint 7500NX	$9	$9	$15	$15

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 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
Check Point 13800	$231,520	$409,154	$177,634	77%
Cisco FirePOWER 8350	$491,121	$711,199	$220,078	45%
Forcepoint Stonesoft 3301	$158,821	$334,375	$175,554	111%
Fortinet FortiGate 3000D	$193,700	$210,132	$16,432	8%
IBM XGS 7100	$942,400	$686,102	-$256,298	-27%
Intel Security McAfee NS9100	$579,023	$360,473	-$218,550	-38%
Palo Alto Networks PA-7050	$3,293,800	$1,227,042	-$2,066,758	-63%
Trend Micro TippingPoint 7500NX	$457,987	$424,771	-$33,216	-7%

Figure 10 – Purchase Price vs. Security Effectiveness Value (US$)

Test Methodology

Next Generation Intrusion Prevention System v2.0

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

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

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.