NEXT GENERATION INTRUSION PREVENTION SYSTEM COMPARATIVE REPORT

Security Value Map™ (SVM)

NOVEMBER 7, 2017

Author – Thomas Skybakmoen

Tested Products

Check Point Software Technologies 15600 R77.30

Cisco FirePOWER 8350 v6.2.0.1

Forcepoint NGFW 3301 v6.2.1

Fortinet FortiGate 600D v5.4.5

IBM QRadar Network Security XGS 5200 v5.4.0

McAfee IPS-NS9100 v9.1.5.3

Palo Alto Networks PA-5250 v8.0.3-h4

Trend Micro 7500NX v3.9.2.4784

Trend Micro 8400TX v5.0.0.4815

Environment

Next Generation Intrusion Prevention System Test Methodology v.3.1

Overview

Empirical data from individual Test Reports and Comparative Reports is used to create NSS Labs' unique Security Value Map™ (SVM). The SVM illustrates the relative value of security investment options by mapping the *Security Effectiveness* and the *Total Cost of Ownership (TCO) per Protected Mbps* (*Value*) of tested product configurations. The terms *TCO per Protected Mbps* and *Value* are used interchangeably throughout the Comparative Reports.

The SVM provides an aggregated view of the detailed findings from NSS' group tests. Individual Test Reports are available for each product tested. Comparative Reports provide detailed comparisons across all tested products in the areas of security, performance, and TCO.

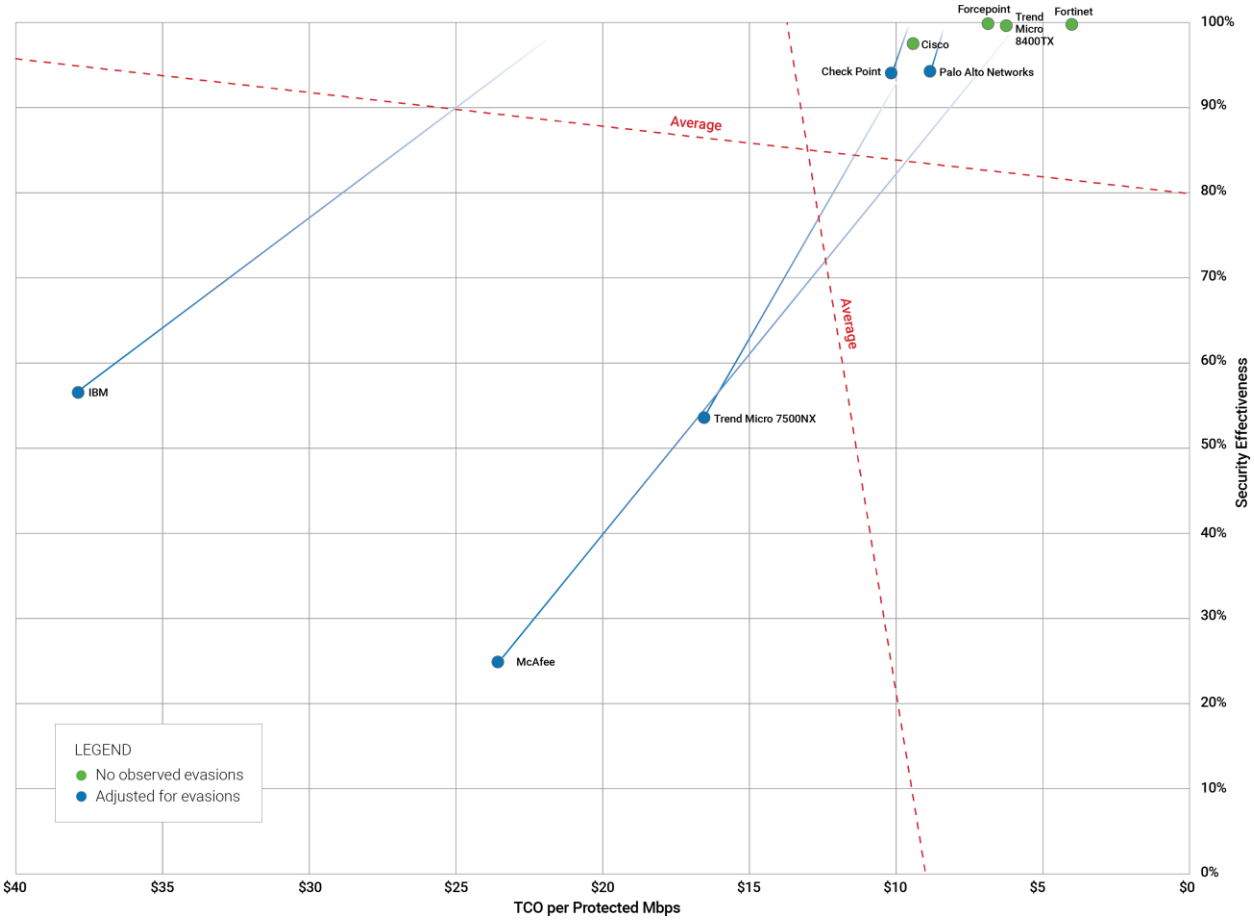

Figure 1 – NSS Labs 2017 Security Value Map (SVM) for Next Generation Intrusion Prevention Systems (NGIPS)

Key Findings

- Six products achieved a *Recommended* rating and three products received a *Caution* rating.
- Five out of the nine products tested missed evasions.
- *Security Effectiveness* ranged between 25.0% and 99.9%.
- The average *Security Effectiveness* rating was 80.0%; six products received a *Security Effectiveness* rating above this average, and three received a *Security Effectiveness* rating below the average.
- *TCO per Protected Mbps* ranged between US$4 and US$38, with most tested products costing less than US$20 per protected Mbps.
- The average *TCO per Protected Mbps* (*Value*) was US$14; six products demonstrated value above the average, and three demonstrated value below the average.
- 157 evasion techniques were utilized in the test.

Product Rating

The Overall Rating in Figure 2 is determined by which section of the SVM the product falls within: *Recommended* (top right), *Neutral* (top left or bottom right), or *Caution* (bottom left). For more information on how the SVM is constructed, see the *How to Read the SVM* section of this document.

Product	Security Effectiveness		Value in US$ (TCO per Protected Mbps)		Overall Rating
Check Point 15600	94.1%	Above average	$10	Above average	Recommended
Cisco FirePOWER 8350	97.4%	Above average	$9	Above average	Recommended
Forcepoint NGFW 3301	99.9%	Above average	$7	Above average	Recommended
Fortinet FortiGate 600D	99.7%	Above average	$4	Above average	Recommended
IBM XGS 5200	56.7%	Below average	$38	Below average	Caution
McAfee NS9100	25.0%	Below average	$24	Below average	Caution
Palo Alto Networks PA-5250	94.3%	Above average	$9	Above average	Recommended
Trend Micro 7500NX	53.6%	Below average	$17	Below average	Caution
Trend Micro 8400TX	99.6%	Above average	$6	Above average	Recommended

Figure 2 – NSS Labs' 2017 Recommendations for Next Generation Intrusion Prevention Systems (NGIPS)

This report is part of a series of Comparative Reports on security, performance, TCO, and the SVM. In addition, NSS clients have access to an NSS Labs *SVM Toolkit™* that allows for the incorporation of organization-specific costs and requirements to create a completely customized SVM. For more information, visit www.nsslabs.com.

Table of Contents

Table of Figures

How to Read the SVM

The SVM depicts the value of a typical deployment of four NGIPS products plus one central management unit (and where necessary, a log aggregation and/or event management unit). Running a multi-device deployment provides a more accurate reflection of cost than running only a single NGIPS.

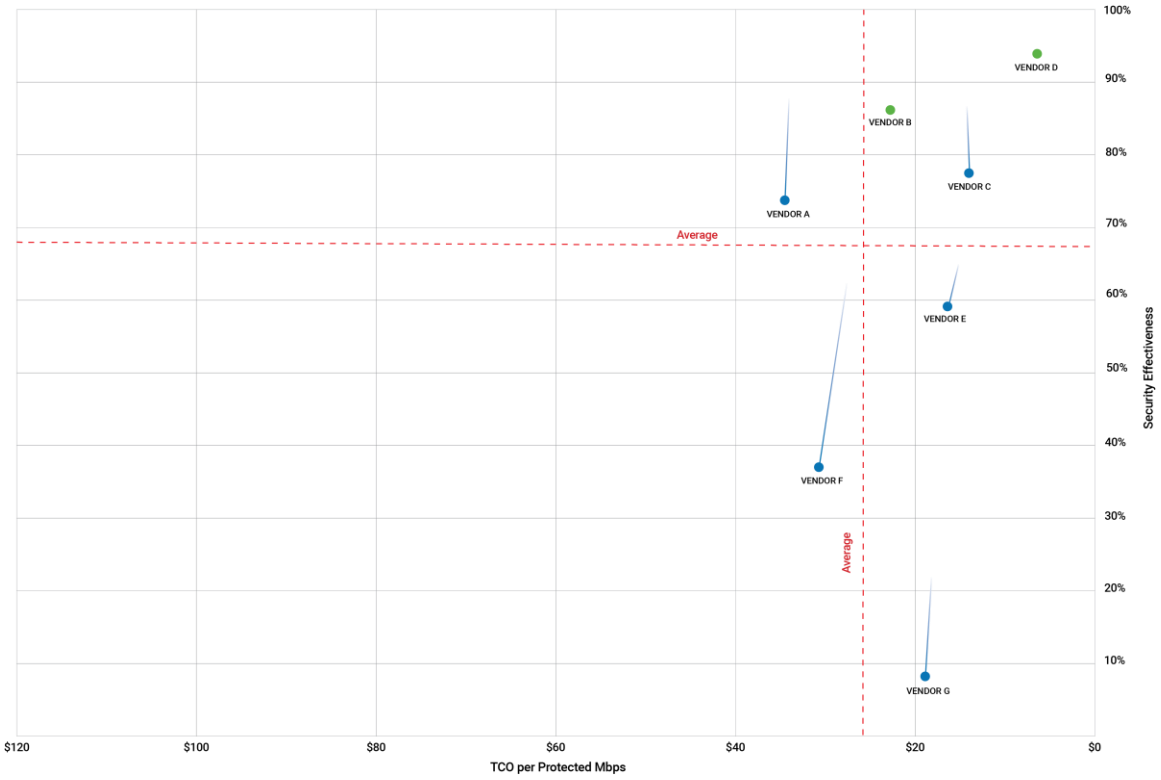

Figure 3 – Example SVM

No two security products 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 metric: *TCO per Protected Mbps.*

The *x* axis displays the *TCO per Protected Mbps* in US dollars, which decreases from left to right. This metric incorporates the 3-Year TCO with the *Security Effectiveness* score to provide a data point with which to compare the actual value of each product tested. The formula used is as follows: 3-Year TCO/ (*Security Effectiveness* x *NSS-Tested Throughput*). The TCO incorporates capital expenditure (capex) costs over a three-year period, including initial acquisition and deployment costs and annual maintenance and update costs (software and hardware updates). For more details on *Security Effectiveness* and TCO, see the Security and TCO comparative reports at www.nsslabs.com.

The *y* axis displays the *Security Effectiveness* score as a percentage. *Security Effectiveness* is greater toward the top of the *y* axis. Devices that are missing critical security capabilities will have a reduced *Security Effectiveness* score.

The *Security Effectiveness* score of some products is represented by two data points (a blue dot and a gradient line). The highest point of the gradient line represents *Security Effectiveness* based solely on block rate. However,

this is not the only measure of S*ecurity Effectiveness*—NSS also factors in evasions. Incorporating this additional information allows NSS to calculate a second, lower score (represented by the blue dot), which more realistically depicts the actual *Security Effectiveness* of a product.

The *Security Effectiveness* score of products that did not miss any evasions is represented by a single green dot.

The SVM displays two dotted lines that represent the average for the *Security Effectiveness* and *TCO per Protected Mbps* ratings of all the tested products. These lines divide the SVM into four unequally sized sections. Where a product's *Security Effectiveness* and *TCO per Protected Mbps* scores map on the SVM will determine which section it falls into:

- **Recommended**: Products that map into the upper-right section of the SVM score well for both *Security Effectiveness* and *TCO per Protected Mbps***.** These products provide a high level of detection and value for money.
- **Caution:** Products that map into the lower-left section of the SVM offer limited value for money given their 3-Year TCO and measured *Security Effectiveness*.
- **Neutral:** Products that map into either the upper-left or lower-right sections may be good choices for organizations with specific security or budget requirements.

Neutral products in the upper-left section score above the average for *Security Effectiveness* but below the average for *TCO per Protected Mbps* (*Security Recommended).* These products are suitable for environments requiring a high level of detection, albeit at a higher-than-average cost.

Conversely, *Neutral* products in the lower-right section score below the average for *Security Effectiveness* but above the average for *TCO per Protected Mbps*. These products would be suitable for environments where a slightly lower level of detection is acceptable in exchange for a lower TCO.

In all cases, the SVM should only be a starting point. NSS clients have access to the *SVM Toolkit*, which allows for the incorporation of organization-specific costs and requirements to create a custom SVM. Clients can also meet with NSS analysts if they wish to develop a custom SVM.

Analysis

Each product may fall into one of three categories based on its rating in the SVM: *Recommended*, *Neutral*, or *Caution*. Each of the tested products receives only a single rating. Vendors are listed alphabetically within each section.

Recommended

Check Point Software Technologies 15600 R77.30

Block Rate	Using the vendor-provided settings, the Check Point 15600 blocked 99.52% of attacks.
Evasion Techniques	The Check Point 15600 blocked 155 out of the 157 evasions it was tested against.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The Check Point 15600 is rated by NSS at 8,691 Mbps, which is higher than the vendor-claimed performance (Check Point rates this device at 8 Gbps).

Cisco FirePOWER 8350 v6.2.0.1

Block Rate	Using the vendor-provided settings, the FirePOWER 8350 blocked 97.39% of attacks.
Evasion Techniques	The device proved to be effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The FirePOWER 8350 is rated by NSS at 19,499 Mbps, which is higher than the vendor-claimed performance (Cisco rates this device at 15 Gbps).

Forcepoint NGFW 3301 v6.2.1

Block Rate	Using the vendor-provided settings, the NGFW 3301 blocked 99.91% of attacks.
Evasion Techniques	The device proved to be effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The NGFW 3301 is rated by NSS at 10,922 Mbps, which is higher than the vendor-claimed performance (Forcepoint rates this device at 9,000 Mbps).

Fortinet FortiGate 600D v5.4.5

Block Rate	Using the vendor-provided settings, the FortiGate 600D blocked 99.72% of attacks.
Evasion Techniques	The device proved to be effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The FortiGate 600D is rated by NSS at 3,707 Mbps, which is lower than the vendor-claimed performance (Fortinet rates this device at 4 Gbps).

Palo Alto Networks PA-5250 v8.0.3-h4

Block Rate	Using the vendor-provided settings, the PA-5250 blocked 99.81% of attacks.
Evasion Techniques	The device blocked 155 out of the 157 evasions it was tested against.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The PA-5250 is rated by NSS at 17,194 Mbps, which is lower than the vendor-claimed performance (Palo Alto Networks rates this device at 20 Gbps).

Trend Micro 8400TX v5.0.0.4815

Block Rate	Using the vendor-provided settings, the Trend Micro 8400TX blocked 99.65% of attacks.
Evasion Techniques	The device proved to be effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The Trend Micro 8400TX is rated by NSS at 36,280 Mbps, which is below the vendor-claimed performance (Trend Micro rates this device at 40 Gbps).

Neutral

No vendor received a Neutral rating.

Caution

IBM QRadar Network Security XGS 5200 v5.4.0

Block Rate	Using the vendor-provided settings, the QRadar Network Security XGS 5200 blocked 98.02% of attacks.
Evasion Techniques	The device blocked 147 out of the 157 evasions it was tested against.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The QRadar Network Security XGS 5200 is rated by NSS at 10,057 Mbps, which is lower than the vendor-claimed performance (IBM rates this device at 12 Gbps).

McAfee IPS-NS9100 v9.1.5.3

Block Rate	Using the vendor-provided settings, the IPS-NS9100 blocked 99.96% of attacks.
Evasion Techniques	The device blocked 135 out of the 157 evasions it was tested against.
Stability and Reliability	The device failed the following stability and reliability test: Blocking Under Extended Attack[1].
Performance Rating	The IPS-NS9100 is rated by NSS at 24,743 Mbps, which is higher than the vendor-claimed performance (McAfee rates this device at 10 Gbps).

Trend Micro 7500NX v3.9.2.4784

Block Rate	Using the vendor-provided settings, the 7500NX blocked 99.75% of attacks.
Evasion Techniques	The device blocked 146 of the 157 evasions it was tested against.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The 7500NX is rated by NSS at 15,959 Mbps, which is below the vendor-claimed performance (Trend Micro rates this device at 20 Gbps).

[1]. The device submitted by McAfee consistently failed our Blocking under Extended Attack test case. However, during testing of a separate device in a different group test, we did not observe this failure—even when using the same version and configuration as was used in the original test. This may indicate that results were specific to the device submitted or that there is a bug, which manifests in certain situations and renders protections unreliable. Enterprises should work with the vendor to ensure that their deployed systems are not exhibiting this behavior.

Test Methodology

Next Generation Intrusion Prevention System Test Methodology v3.1

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

Contact Information

NSS Labs, Inc.
3711 South MoPac Expressway
Building 1, Suite 400
Austin, TX 78746-8022
USA
info@nsslabs.com
www.nsslabs.com