NEXT GENERATION INTRUSION PREVENTION SYSTEM COMPARATIVE REPORT

Security Value Map™ (SVM)

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 v.2.0

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 following areas:

- Security
- Performance
- TCO

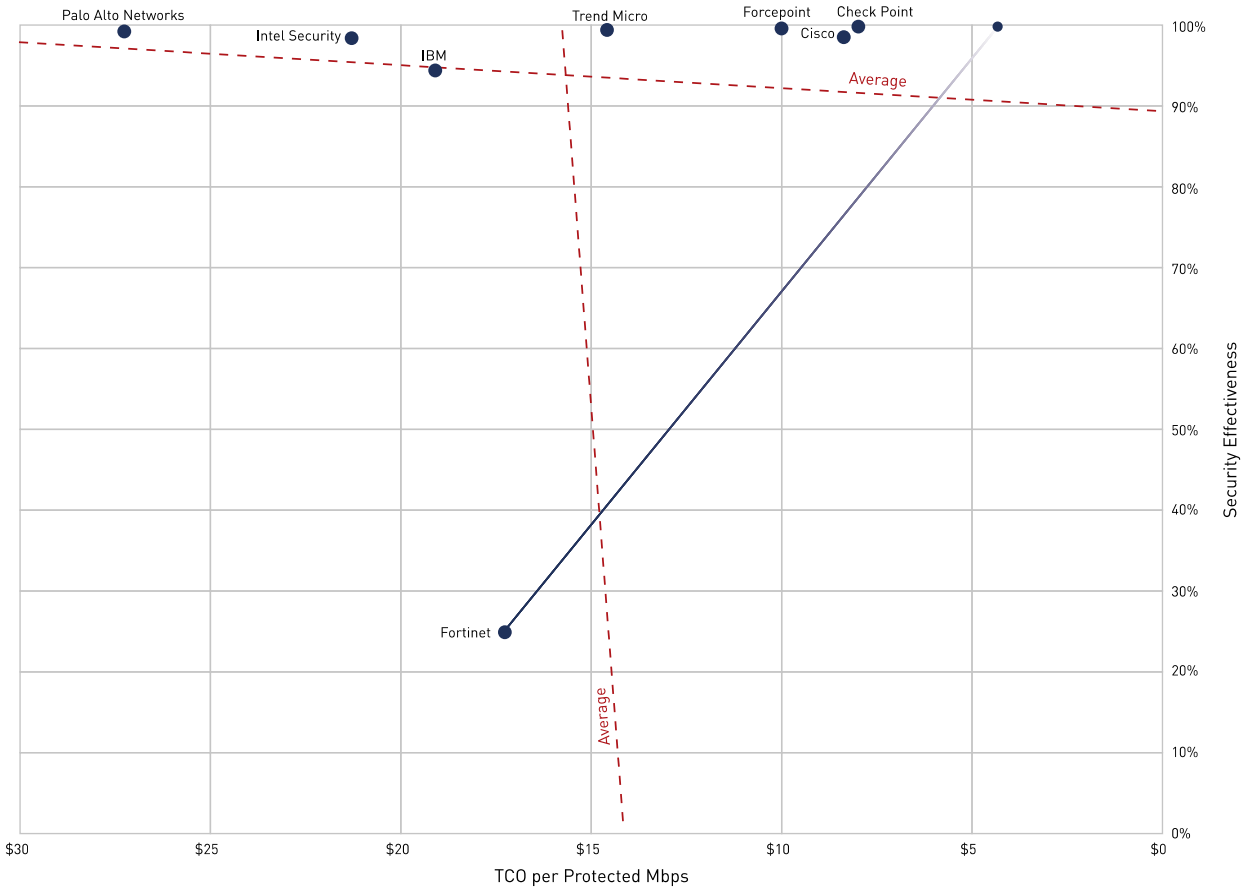

Figure 1 – NSS Labs' 2016 Security Value Map (SVM) for Next Generation Intrusion Prevention Systems (NGIPS)

Key Findings

- Overall *Security Effectiveness* ranged between 24.9% and 99.9%, with four of the eight tested products achieving a rating greater than 99.0%.
- *TCO per Protected Mbps* ranged between US$8 and US$27, with most of the products tested costing less than US$18 per protected Mbps.
- The average *TCO per Protected Mbps* was US$16; four devices were rated as having above-average value, and four were rated as having below-average value.
- 120 evasion techniques were utilized in the test.
- 2,577,402 suspicious URLs yielded more than 2,400 drive-by exploits used by threat actors in active campaigns at the time of testing, which makes this the largest live test ever conducted.
- Active drive-by exploits were tested for up to three days, which resulted in 48,488 discrete test cases across more than 7,000 live victim machines.

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 13800	99.9%	Above Average	$8.04	Above Average	Recommended
Cisco FirePOWER 8350	98.7%	Above Average	$8.42	Above Average	Recommended
Forcepoint Stonesoft 3301	99.6%	Above Average	$10.03	Above Average	Recommended
Fortinet FortiGate 3000D	24.9%	Below Average	$17.33	Below Average	Caution
IBM XGS 7100	94.4%	Below Average	$19.13	Below Average	Caution
Intel Security McAfee NS9100	98.5%	Above Average	$21.34	Below Average	Neutral
Palo Alto Networks PA-7050	99.3%	Above Average	$27.28	Below Average	Neutral
Trend Micro TippingPoint 7500NX	99.5%	Above Average	$14.63	Above Average	Recommended

Figure 2 – NSS Labs' 2016 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.

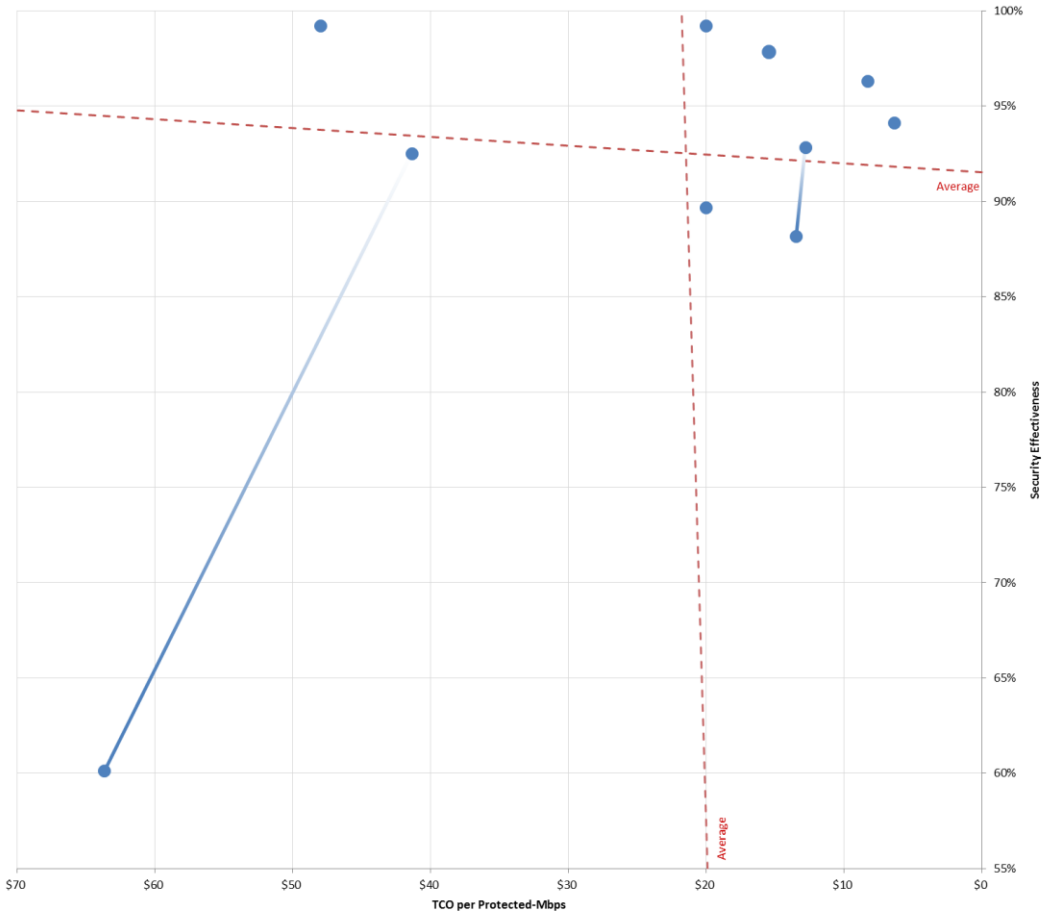

Figure 3 – Example SVM

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 against from which the actual value of each product tested can be compared. 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 SVM displays two dotted lines that represent the average *Security Effectiveness* and *TCO per Protected Mbps* 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 as above average for *Security Effectiveness* but below average for *TCO per Protected Mbps (Value)*. 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 as below average for *Security Effectiveness* but above average for *TCO per Protected Mbps (Value)*. These products would be suitable for environments where a slightly lower level of detection is acceptable in exchange for a lower TCO.

Note that in cases where a product is represented by two dots, the upper dot reflects the product's optimum security capability while the lower dot takes into account how the product was rated if it missed a test category such as evasions, application control, or stability and reliability. The lower dot reflects the product's final rating in the SVM.

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, Ltd. 13800 Next Generation Firewall Appliance vR77.20

Block Rate	Using a recommended policy, the Check Point Software Technologies 13800 Next Generation Firewall Appliance blocked 100.0% of attacks against server applications, 99.9% of attacks against client applications, and 99.9% of attacks overall.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Application Control	NSS engineers verified that the product successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The device is rated by NSS at 12,345 Mbps, which is higher than the vendor-claimed performance (Check Point rates this device at 6.4 Gbps).

Cisco FirePOWER 8350 v6.0.1

Block Rate	Using a recommended policy, the Cisco FirePOWER 8350 blocked 99.0% of attacks against server applications, 98.5% of attacks against client applications, and 98.7% of attacks overall.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Application Control	NSS engineers verified that the product successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The device is rated by NSS at 21,713 Mbps, which is higher than the vendor-claimed performance (Cisco rates this device at 15 Gbps).

Forcepoint Stonesoft Next Generation Firewall 3301 v6.0.2

Block Rate	Using a recommended policy, the Forcepoint Stonesoft NGFW 3301 blocked 100.0% of attacks against server applications, 99.8% of attacks against client applications, and 99.9% of attacks overall.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Application Control	NSS engineers verified that the product successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The device is rated by NSS at 10,110 Mbps, which is higher than the vendor-claimed performance (Forcepoint rates this device at 8 Gbps).

Trend Micro TippingPoint 7500NX v3.8.4.4525

Block Rate	Using a recommended policy, the Trend Micro TippingPoint 7500NX blocked 99.3% of attacks against server applications, 99.3% of attacks against client applications, and 99.3% of attacks overall.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Application Control	NSS engineers verified that the product successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The device is rated by NSS at 12,856 Mbps, which is lower than the vendor-claimed performance (Trend Micro rates this device at 20 Gbps).

Neutral

Intel Security McAfee Network Security Platform NS9100 v8.2.5.158

Block Rate	Using a recommended policy, the Intel Security McAfee Network Security Platform NS9100 blocked 99.6% of attacks against server applications, 99.9% of attacks against client applications, and 99.7% of attacks overall.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Application Control	NSS engineers verified that the product successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The device is rated by NSS at 11,023 Mbps, which is higher than the vendor-claimed performance (Intel Security rates this device at 10,000 Mbps).

Palo Alto Networks PA-7050 v7.0.4

Block Rate	Using a recommended policy, the Palo Alto Networks PA-7050 blocked 98.5% of attacks against server applications, 99.2% of attacks against client applications, and 98.8% of attacks overall.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Application Control	NSS engineers verified that the product successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The device is rated by NSS at 37,238 Mbps, which is lower than the vendor-claimed performance (Palo Alto Networks rates this device at 60 Gbps).

Caution

Fortinet FortiGate 3000D v5.4.0

Block Rate	Using a recommended policy, the Fortinet FortiGate 3000D blocked 99.5% of attacks against server applications, 99.7% of attacks against client applications, and 99.6% of attacks overall.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device failed the following stability and reliability test: State Preservation – Maximum Exceeded.
Application Control	NSS engineers verified that the product successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The device is rated by NSS at 25,386 Mbps, which is higher than the vendor-claimed performance (Fortinet rates this device at 25,000 Mbps).

IBM Security Network Protection XGS 7100 v5.3.2.1

Block Rate	Using a recommended policy, the IBM Security Network Protection XGS 7100 blocked 96.8% of attacks against server applications, 97.1% of attacks against client applications, and 97.0% of attacks overall.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Application Control	NSS engineers verified that the product successfully determined the correct application and took the appropriate action based on the policy.

Performance Rating	The device is rated by NSS at 21,886 Mbps, which is lower than the vendor-claimed performance (IBM rates this device at 25 Gbps).

Test Methodology

Next Generation Intrusion Prevention System Test Methodology 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