NEXT GENERATION FIREWALL COMPARATIVE REPORT

Security Value Map™ (SVM)

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

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 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 and can be found at www.nsslabs.com. Comparative Reports provide detailed comparisons across all tested products in the following areas:

- Security
- Performance
- TCO

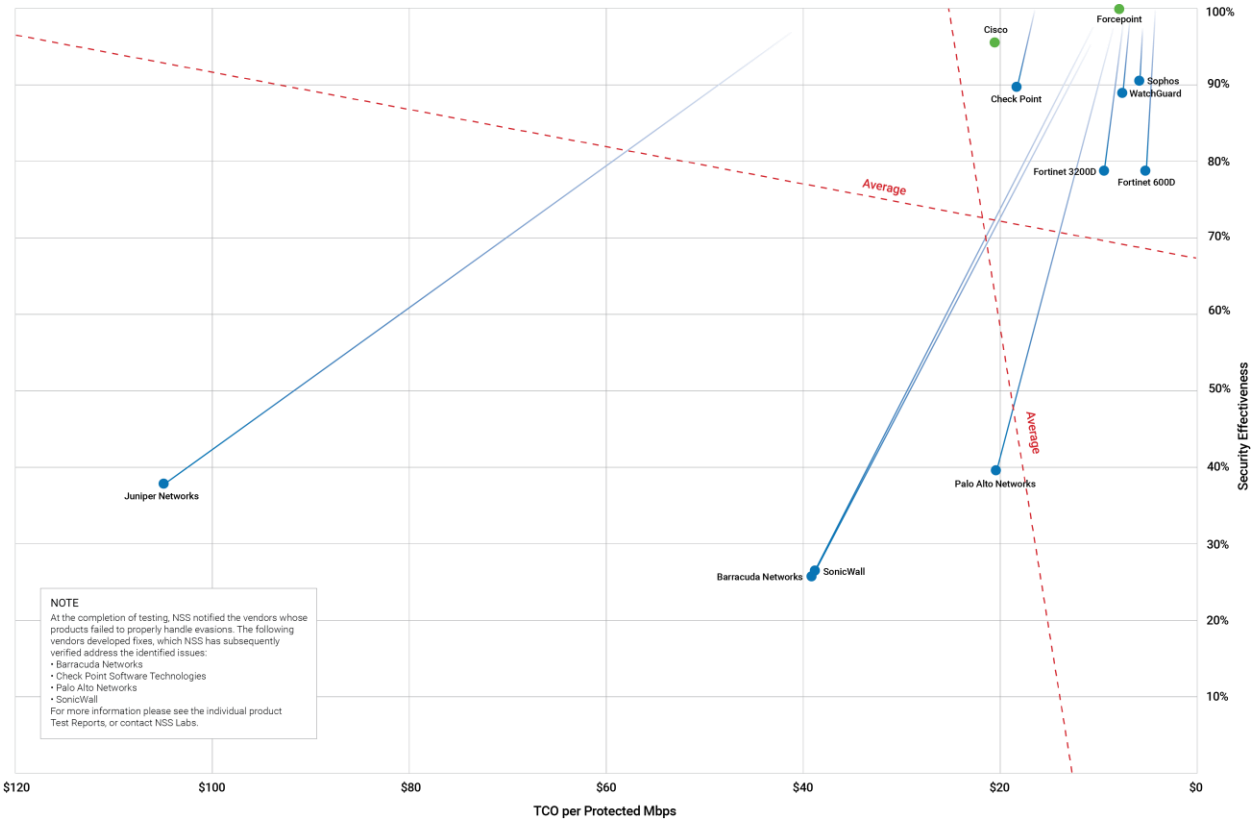

Figure 1 – NSS Labs' 2017 Security Value Map™ (SVM) for Next Generation Firewall (NGFW)

Key Findings

- Overall *Security Effectiveness* ranged from 25.8% to 99.9%, with seven of the 11 tested products achieving a rating greater than 78.5%.
- *TCO per Protected Mbps* ranged from US$5 to US$105, with most tested products costing less than US$22 per protected Mbps.
- The average *Security Effectiveness* rating was 67.3%; seven of the tested products received an above-average *Security Effectiveness* rating, and four of the tested products received a below-average *Security Effectiveness* rating.
- The average *TCO per Protected Mbps* was US$25.2; eight of the tested products were rated as having above-average value, and three of the tested products were rated as having below-average value.

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.

Vendor	Security Effectiveness		Value (TCO per Protected Mbps)		Overall Rating
Barracuda Networks	25.8%	Below Average	US$39	Below Average	Caution
Check Point	89.6%	Above Average	US$18	Above Average	Recommended
Cisco	95.5%	Above Average	US$21	Above Average	Recommended
Forcepoint	99.9%	Above Average	US$8	Above Average	Recommended
Fortinet 3200D	78.6%	Above Average	US$9	Above Average	Recommended
Fortinet 600D	78.6%	Above Average	US$5	Above Average	Recommended
Juniper Networks	37.8%	Below Average	US$105	Below Average	Caution
Palo Alto Networks	39.7%	Below Average	US$20	Above Average	Caution
SonicWall	26.4%	Below Average	US$39	Below Average	Caution
Sophos	90.4%	Above Average	US$6	Above Average	Recommended
WatchGuard	88.9%	Above Average	US$8	Above Average	Recommended

Figure 2 – NSS Labs' 2017 Recommendations for Next Generation Firewall (NGFW)

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 five (5) NGFW devices plus one (1) 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 NGFW device.

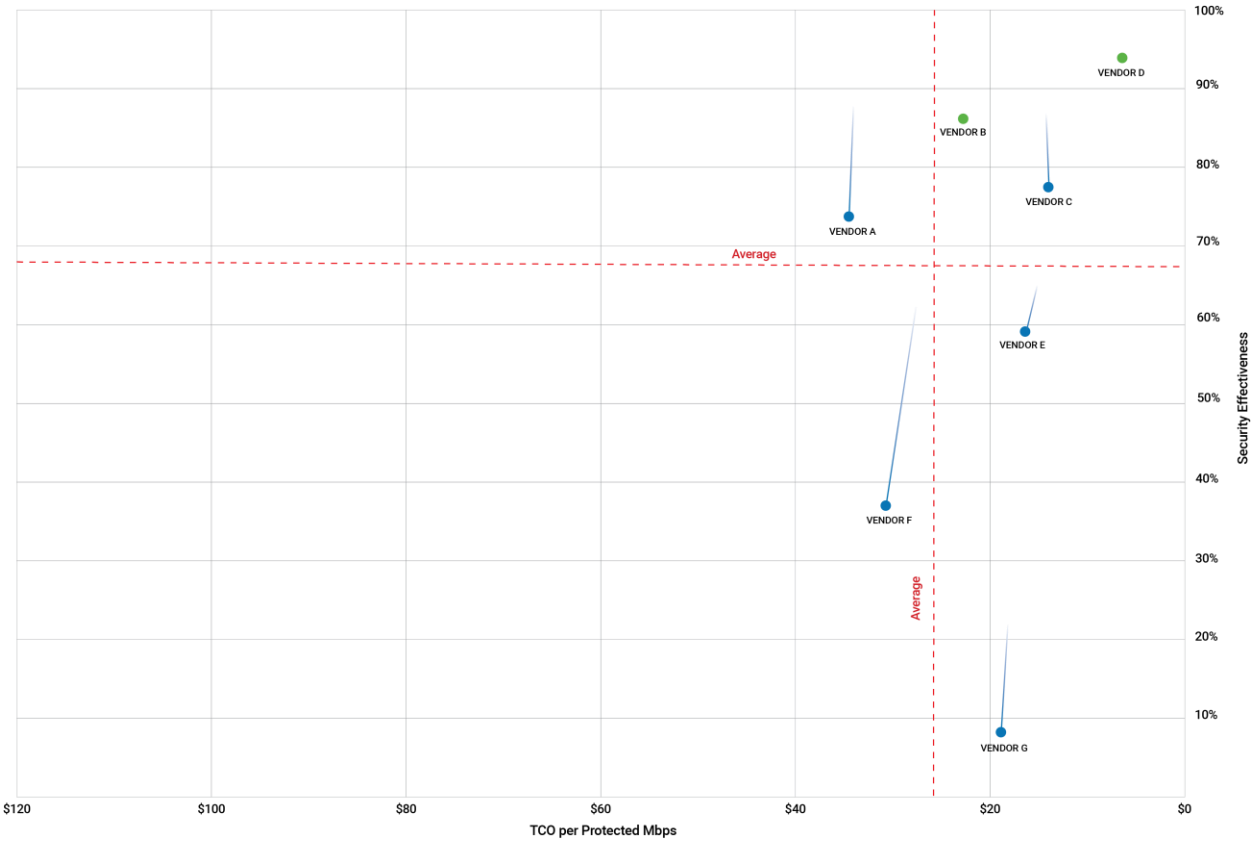

Figure 3 – Example SVM

No two security products deliver the same security effectiveness or TCO, making precise comparisons extremely difficult. In order to enable value-based comparisons of NGFW products on the market, NSS has developed a unique metric: *TCO per Protected Mbps*. For additional information, please see the TCO Comparative Report.

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 which the actual value of each product tested can be compared. The following formula is used: *TCO per Protected Mbps* = 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. Products that are missing critical security capabilities will have reduced *Security Effectiveness* scores.

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 *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 *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.

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 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 a single rating. Vendors are listed alphabetically within each section.

Recommended

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

***NSS Exploit Library* Block Rate**	Using the recommended policy, the 15600 NGTP Appliance blocked 99.90% of attacks against server applications, 99.82% of attacks against client applications, and 99.86% of attacks overall.
CAWS (Live) Exploit Block Rate	The device blocked 99.27% of live exploits.
Evasion Techniques	The device failed to protect against the HTTP evasion technique. Please see the Test Report for additional details.
Stability and Reliability	The device passed all stability and reliability tests.
Firewall Policy Enforcement	The device proved effective in enforcing all firewall policies.
Application Control	NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The 15600 NGTP Appliance is rated by NSS at 5,516 Mbps, which is higher than the vendor-claimed performance; Check Point rates this device at 5.2 Gbps.

Cisco Firepower 4110 v6.1.0.1

***NSS Exploit Library* Block Rate**	Using the recommended policy, the Firepower 4110 blocked 97.43% of attacks against server applications, 98.84% of attacks against client applications, and 98.19% of attacks overall.
CAWS (Live) Exploit Block Rate	The device blocked 92.81% of live exploits.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Firewall Policy Enforcement	The device proved effective in enforcing all firewall policies.
Application Control	NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The Firepower 4110 is rated by NSS at 2,495 Mbps, which is lower than the vendor-claimed performance; Cisco rates this device at 10 Gbps.

Forcepoint NGFW 3301 Appliance v6.1.2

***NSS Exploit Library* Block Rate**	Using the recommended policy, the NGFW 3301 Appliance blocked 100.0% of attacks against server applications, 100.00% of attacks against client applications, and 100.0% of attacks overall.
CAWS (Live) Exploit Block Rate	The device blocked 99.89% of live exploits.
Evasion Techniques	The device proved effective against all evasion techniques tested.
Stability and Reliability	The device passed all stability and reliability tests.
Firewall Policy Enforcement	The device proved effective in enforcing all firewall policies.
Application Control	NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The Forcepoint 3301 Appliance is rated by NSS at 9,952 Mbps, which is higher than the vendor-claimed performance; Forcepoint rates this device at 9 Gbps.

Fortinet FortiGate 3200D FortiOS v5.4.4 GA Build 1117

***NSS Exploit Library* Block Rate**	Using the recommended policy, the FortiGate 3200D blocked 99.90% of attacks against server applications, 98.66% of attacks against client applications, and 99.24% of attacks overall.
CAWS (Live) Exploit Block Rate	The device blocked 99.71% of live exploits.
Evasion Techniques	The device failed to protect against the HTML obfuscation evasion technique. Please see the Test Report for additional details.
Stability and Reliability	The device passed all stability and reliability tests.
Firewall Policy Enforcement	The device proved effective in enforcing all firewall policies.
Application Control	NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The FortiGate 3200D is rated by NSS at 18,573 Mbps, which is lower than the vendor-claimed performance; Fortinet rates this device at 24 Gbps.

Fortinet FortiGate 600D FortiOS v5.4.4 GA Build 1117

***NSS Exploit Library* Block Rate**	Using the recommended policy, the FortiGate 3200D blocked 99.90% of attacks against server applications, 98.66% of attacks against client applications, and 99.24% of attacks overall.
CAWS (Live) Exploit Block Rate	The device blocked 99.71% of live exploits.
Evasion Techniques	The device failed to protect against the HTML obfuscation evasion technique. Please see the Test Report for additional details.
Stability and Reliability	The device passed all stability and reliability tests.
Firewall Policy Enforcement	The device proved effective in enforcing all firewall policies.
Application Control	NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The FortiGate 600D is rated by NSS at 3,688 Mbps, which is higher than the vendor-claimed performance; Fortinet rates this device at 3.2 Gbps

Sophos XG-750 Firewall v16.01

***NSS Exploit Library* Block Rate**	Using the recommended policy, the XG-750 Firewall blocked 96.30% of attacks against server applications, 93.05% of attacks against client applications, and 94.56% of attacks overall.
CAWS (Live) Exploit Block Rate	The device blocked 97.82% of live exploits.
Evasion Techniques	The device failed to protect against the HTML obfuscation evasion technique. Please see the Test Report for additional details.
Stability and Reliability	The device passed all stability and reliability tests.
Firewall Policy Enforcement	The device proved effective in enforcing all firewall policies.
Application Control	NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The XG-750 Firewall is rated by NSS at 8,628 Mbps, which is lower than the vendor-claimed performance; Sophos rates this device at 11.8 Gbps.

WatchGuard Firebox M4600 v11.10.7

***NSS Exploit Library* Block Rate**	Using the recommended policy, the Firebox M4600 blocked 97.13% of attacks against server applications, 98.04% of attacks against client applications, and 97.62% of attacks overall.
CAWS (Live) Exploit Block Rate	The device blocked 99.87% of live exploits.
Evasion Techniques	The device failed to protect against the HTTP evasion technique. Please see the Test Report for additional details.
Stability and Reliability	The device passed all stability and reliability tests.
Firewall Policy Enforcement	The device proved effective in enforcing all firewall policies.
Application Control	NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The Firebox M4600 is rated by NSS at 2,472 Mbps, which is lower than the vendor-claimed performance; WatchGuard rates this device at 3 Gbps.

Neutral

No vendor received a *Neutral* rating.

Caution

Barracuda NextGen Firewall F600.E20 Firmware Version 7.0.2

***NSS Exploit Library* Block Rate**	Using the recommended policy, the Barracuda NextGen Firewall F600.E20 blocked 89.73% of attacks against server applications, 96.62% of attacks against client applications, and 93.42% of attacks overall.
CAWS (Live) Exploit Block Rate	The device blocked 97.84% of live exploits.
Evasion Techniques	The device failed to protect against the HTTP evasion technique. Please see the Test Report for additional details.
Stability and Reliability	The device passed all stability and reliability tests.
Firewall Policy Enforcement	The device proved effective in enforcing all firewall policies.
Application Control	NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The Barracuda NextGen Firewall F600.E20 is rated by NSS at 2,842 Mbps, which is higher than the vendor-claimed performance; Barracuda Networks rates this device at 2.6 Gbps.

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

***NSS Exploit Library* Block Rate**	Using the recommended policy, the SRX 4200 blocked 98.77% of attacks against server applications, 99.64% of attacks against client applications, and 99.24% of attacks overall.
CAWS (Live) Exploit Block Rate	The device blocked 94.86% of live exploits.
Evasion Techniques	The device failed to protect against the RPC fragmentation, HTML obfuscation, and HTTP evasion techniques. Please see the Test Report for additional details.
Stability and Reliability	The device passed all stability and reliability tests.
Firewall Policy Enforcement	The device proved effective in enforcing all firewall policies.
Application Control	NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The SRX 4200 is rated by NSS at 1,955 Mbps, which is lower than the vendor-claimed performance; Juniper rates this device at 15 Gbps.

Palo Alto Networks PA-5250 PAN-OS 8.0.0

***NSS Exploit Library* Block Rate**	Using the recommended policy, the PA-5250 blocked 98.77% of attacks against server applications, 99.47% of attacks against client applications, and 99.14% of attacks overall.
CAWS (Live) Exploit Block Rate	The device blocked 99.58% of live exploits.
Evasion Techniques	The device failed to protect against the HTTP evasion technique. Please see the Test Report for additional details.
Stability and Reliability	The device passed all stability and reliability tests.
Firewall Policy Enforcement	The device proved effective in enforcing all firewall policies.
Application Control	NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The PA-5250 is rated by NSS at 17,740 Mbps, which is lower than the vendor-claimed performance; Palo Alto Networks rates this device at 20.3 Gbps.

SonicWall NSA 6600 SonicOS 6.2

***NSS Exploit Library* Block Rate**	Using the recommended policy, the NSA 6600 blocked 95.38% of attacks against server applications, 96.71% of attacks against client applications, and 96.09% of attacks overall.
CAWS (Live) Exploit Block Rate	The device blocked 99.76% of live exploits.
Evasion Techniques	The device failed to protect against the HTTP evasion technique. Please see the Test Report for additional details.
Stability and Reliability	The device passed all stability and reliability tests.
Firewall Policy Enforcement	The device proved effective in enforcing all firewall policies.
Application Control	NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy.
Performance Rating	The NSA 6600 is rated by NSS at 3,772 Mbps, which is higher than the vendor-claimed performance; SonicWall rates this device at 3 Gbps.

Test Methodology

Next Generation Firewall (NGFW) 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

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