NEXT GENERATION FIREWALL COMPARATIVE REPORT

Security Value Map™ (SVM)

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 NS*a* 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

Unverified Products[1]

Juniper Networks

Huawei

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

[1] NSS was unable to measure the effectiveness and determine the suitability of NGFW products from Juniper Networks and Huawei and therefore cautions against their deployment without a comprehensive evaluation.

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 investments 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

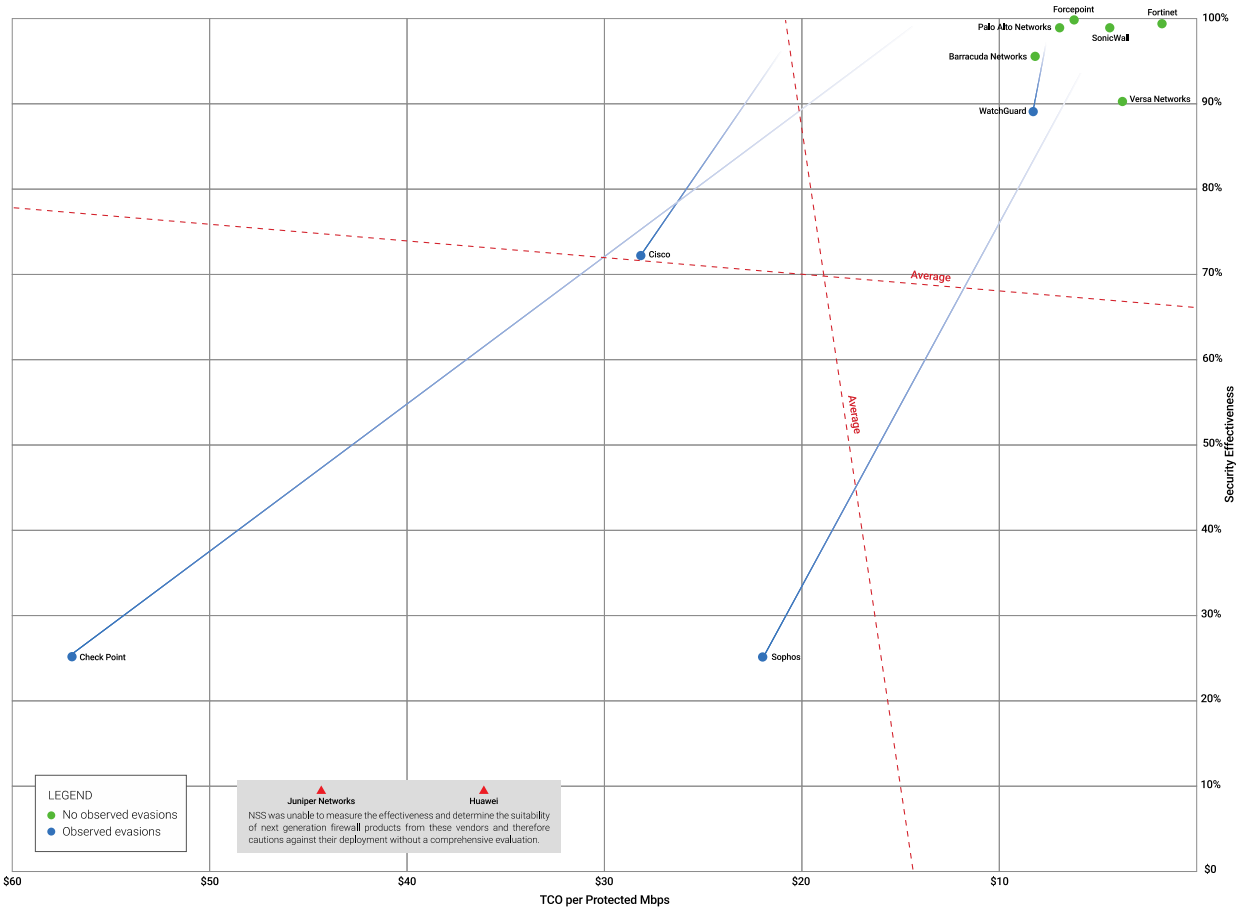

Figure 1 – NSS Labs' 2018 Security Value Map™ (SVM) for Next Generation Firewall (NGFW)

Key Findings

- Overall *Security Effectiveness* ranged from 25.0% to 99.7%, with six of the 10 tested products achieving a rating greater than 90.3%.
- *TCO per Protected Mbps* ranged from US$2 to US$57, with most tested products costing less than US$10 per protected Mbps.
- The average *Security Effectiveness* rating was 66.1%; eight of the tested products received an above-average *Security Effectiveness* rating, and two of the tested products received a below-average *Security Effectiveness* rating.
- The average *TCO per Protected Mbps* was US$20.86; seven of the tested products were rated as having above-average value, and three of the tested products were rated as having below-average value.
- Four tested products missed at least one evasion.
- Of the products tested, none demonstrated full resilience against tested attack variants.

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	95.4%	Above Average	US$8	Above Average	Recommended
Check Point	25.0%	Below Average	US$57	Below Average	Caution
Cisco	71.8%	Above Average	US$28	Below Average	Security Recommended
Forcepoint	99.7%	Above Average	US$6	Above Average	Recommended
Fortinet	99.3%	Above Average	US$2	Above Average	Recommended
Palo Alto Networks	98.7%	Above Average	US$7	Above Average	Recommended
SonicWall	98.8%	Above Average	US$4	Above Average	Recommended
Sophos	25.0%	Below Average	US$22	Below Average	Caution
Versa Networks	90.4%	Above Average	US$4	Above Average	Recommended
WatchGuard	89.1%	Above Average	US$8	Above Average	Recommended

Figure 2 – NSS Labs' 2018 Recommendations for Next Generation Firewall (NGFW)

This report is part of a series of Comparative Reports on security, performance, TCO, and the NSS Labs Security Value Map™ (SVM) In addition, NSS clients have access to an NSS Labs SVM Toolkit™, which 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.

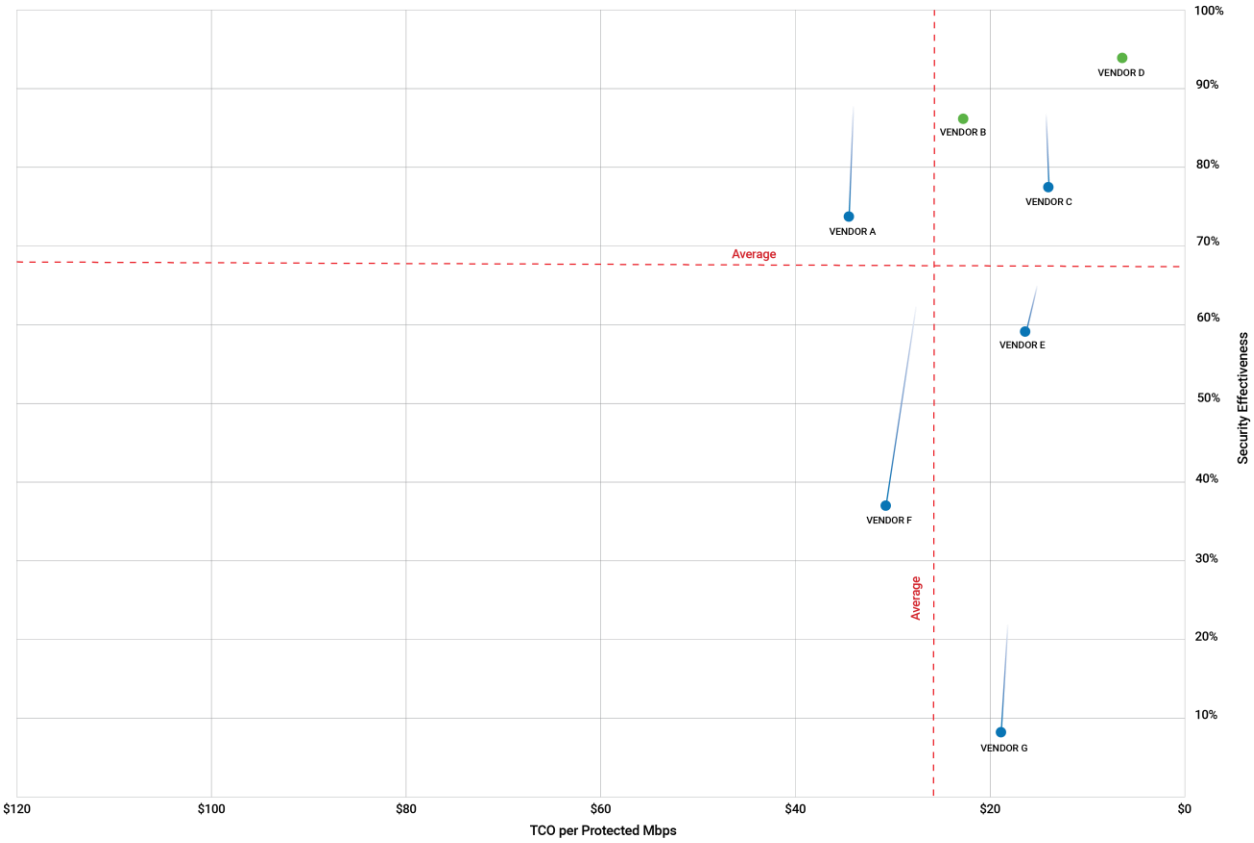

Figure 3 – Example SVM

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 Comparative Reports on Security and TCO 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 and stability and reliability. 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.
- **Security Recommended:** Products that map into the upper-left section of the SVM are suitable for environments requiring a high level of protection, albeit at a higher-than-average cost.
- **Neutral:** Products that map into the lower-right section of the SVM may be good choices for organizations where a slightly lower level of protection is acceptable in exchange for a lower TCO.
- **Caution:** Products that map into the lower-left section of the SVM offer limited value for money given their three-year TCO and measured *Security Effectiveness*.

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

Recommended

Barracuda Networks CloudGen Firewall F800.CCE v7.2.0

***Exploit* Block Rate**	Using the recommended policy, the CloudGen Firewall F800.CCE blocked 95.39% of attacks.
Evasion Techniques	The device proved effective against 190 out of 190 evasions tested. Please see the Test Report for additional details.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The device is rated by NSS at 5,037 Mbps, which is lower than the vendor-claimed performance; Barracuda Networks rates this device at 7,700 Mbps.

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

***Exploit* Block Rate**	Using the recommended policy, the NGFW 2105 Appliance blocked 99.69% of attacks.
Evasion Techniques	The device proved effective against 190 out of 190 evasions tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The device is rated by NSS at 7,654 Mbps, which is higher than the vendor-claimed performance; Forcepoint rates this device at 7,500 Mbps.

Fortinet FortiGate 500E V5.6.3GA build 7858

***Exploit* Block Rate**	Using the recommended policy, the FortiGate 500E blocked 99.31% of attacks.
Evasion Techniques	The device proved effective against 190 out of 190 evasions tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The device is rated by NSS at 6,753 Mbps, which is higher than the vendor-claimed performance; Fortinet rates this device at 5,200 Mbps.

Palo Alto Networks PA-5220 PAN-OS 8.1.1

***Exploit* Block Rate**	Using the recommended policy, the PA-5220 blocked 98.73% of attacks.
Evasion Techniques	The device proved effective against 190 out of 190 evasions tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The device is rated by NSS at 7,888 Mbps, which is lower than the vendor-claimed performance; Palo Alto Networks rates this device at 9,000 Mbps.

SonicWall NS*a* 2650 SonicOS Enhanced 6.5.0.10-73n

***Exploit* Block Rate**	Using the recommended policy, the NSA 2650 blocked 98.77% of attacks.
Evasion Techniques	The device proved effective against 190 out of 190 evasions tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The device is rated by NSS at 1,028 Mbps, which is lower than the vendor-claimed performance; SonicWall rates this device at 1,400 Mbps.

Versa Networks FlexVNF 16.1R1-S6

***Exploit* Block Rate**	Using the recommended policy, the FlexVNF blocked 90.36% of attacks.
Evasion Techniques	The device proved effective against 190 out of 190 evasions tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The device is rated by NSS at 3,661 Mbps, which is lower than the vendor-claimed performance; Versa Networks rates this device at 20,000 Mbps.

WatchGuard M670 v12.0.1.B562953

***Exploit* Block Rate**	Using the recommended policy, the M670 blocked 97.20% of attacks.
Evasion Techniques	The device proved effective against 189 out of 190 evasions tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The device is rated by NSS at 1,589 Mbps, which is lower than the vendor-claimed performance; WatchGuard rates this device at 2,400 Mbps.

Security Recommended

Cisco Firepower 4120 Security Appliance v6.2.2

***Exploit* Block Rate**	Using the recommended policy, the Firepower 4120 Security Appliance blocked 95.70% of attacks.
Evasion Techniques	The device proved effective against 187 out of 190 evasions tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The device is rated by NSS at 5,291 Mbps, which is lower than the vendor-claimed performance; Cisco rates this device at 15,000 Mbps.

Caution

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

***Exploit* Block Rate**	Using the recommended policy, the 15600 Next Generation Threat Prevention (NGTP) Appliance blocked 99.16% of attacks.
Evasion Techniques	The device proved effective against 185 out of 190 evasions tested.
Stability and Reliability	The device did not pass all stability and reliability tests.
Performance Rating	The device is rated by NSS at 5,599 Mbps, which is higher than the vendor-claimed performance; Check Point rates this device at 5,200 Mbps.

Sophos XG Firewall 750 SFOS v17 MR7

***Exploit* Block Rate**	Using the recommended policy, the XG Firewall 750 blocked 93.47% of attacks.
Evasion Techniques	The device proved effective against 178 out of 190 evasions tested.
Stability and Reliability	The device passed all stability and reliability tests.
Performance Rating	The device is rated by NSS at 5,844 Mbps, which is lower than the vendor-claimed performance; Sophos rates this device at 11,800 Mbps.

Juniper Networks

NSS was unable to measure the effectiveness and determine the suitability of NGFW products from this vendor and therefore cautions against their deployment without a comprehensive evaluation.

Huawei

NSS was unable to measure the effectiveness and determine the suitability of NGFW products from this vendor and therefore cautions against their deployment without a comprehensive evaluation.

Neutral

No vendor received a *Neutral* rating.

Test Methodology

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

NSS Labs SSL/TLS Performance Test Methodologyv1.3

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