# NEXT GENERATION FIREWALL COMPARATIVE REPORT

## Security Value Map™ (SVM)

**Authors – Thomas Skybakmoen, Christopher Conrad**

## Tested Products

Barracuda Networks F600.E20 v6.1.1-071

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

Cisco ASA 5585-X SSP-60 v5.4.0.3

Cisco FirePOWER Appliance 8350 v5.4.0.3

Cyberoam – Cyberoam CR2500iNG-XP v10.6.3

Dell SonicWALL SuperMassive E10800 SonicOS Enhanced v6.0.1.13-177o

Forcepoint Stonesoft Next-Generation Firewall 1402 v5.8.5

Fortinet FortiGate 3200D v5.2.4, build 5069

Hillstone Networks SG-6000-E5960 v5.5 SG6000-M-2-5.5R1P2.2

Huawei Technologies USG6650 vV500R001C00SPC010T

Juniper Networks SRX5400E JUNOS Software Release v12.3X48

Palo Alto Networks PA-7050 v6.0.11-h1

WatchGuard Technologies XTM 1525 v11.9.4 build 486684

## Environment

Next Generation Firewall: Test Methodology v6.0

# 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

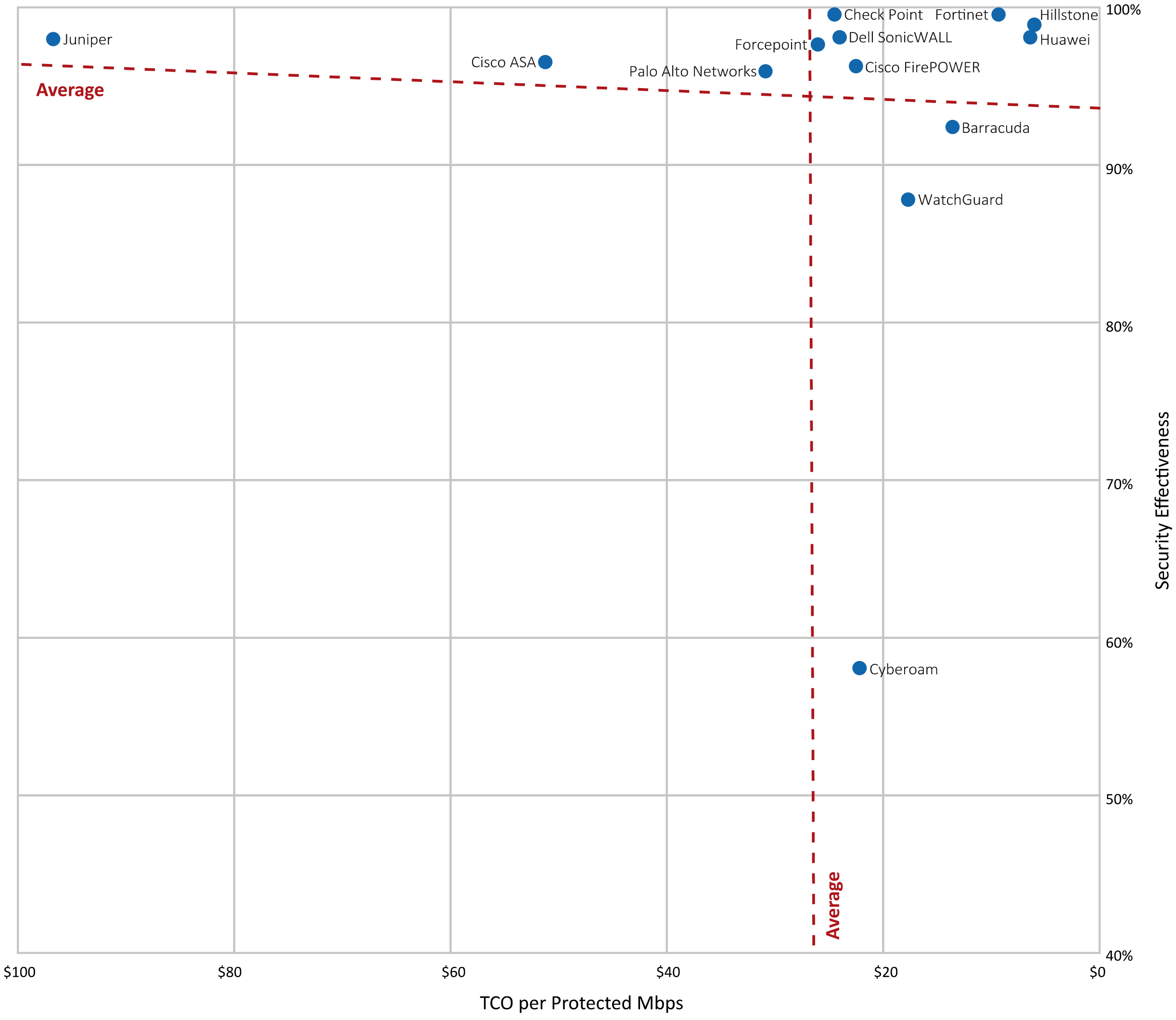

**Figure 1 – NSS Labs 2016 Security Value Map (SVM) for Next Generation Firewall (NGFW)**

## Key Findings

- Overall *Security Effectiveness* ranged between 58.1% and 99.6%, with 10 of the 13 tested products achieving a rating greater than 95%.
- *TCO per Protected Mbps* ranged between US$6 and US$97, with most tested products costing less than US$25 per protected Mbps.
- The average *Security Effectiveness* rating was 93.6%; 10 devices received an above-average *Security Effectiveness* rating, and 3 received a below-average *Security Effectiveness* rating.
- The average *TCO per Protected Mbps* was US$27.20; 10 devices were rated as having above-average value, and 3 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.

| Product | Security Effectiveness | | Value in US$ (TCO per Protected Mbps) | | Overall Rating |
|---|---|---|---|---|---|
| Barracuda Networks F600.E20 | 92.4% | Below Average | $14 | Above Average | Neutral |
| Check Point 13800 NGFW Appliance | 99.6% | Above Average | $25 | Above Average | Recommended |
| Cisco ASA 5585-X SSP-60 | 96.5% | Above Average | $51 | Below Average | Neutral |
| Cisco FirePOWER Appliance 8350 | 96.3% | Above Average | $23 | Above Average | Recommended |
| Cyberoam CR2500iNG-XP | 58.1% | Below Average | $22 | Above Average | Neutral |
| Dell SonicWALL SuperMassive E10800 | 98.1% | Above Average | $24 | Above Average | Recommended |
| Forcepoint Stonesoft NGFW 1402 | 97.6% | Above Average | $26 | Above Average | Recommended |
| Fortinet FortiGate 3200D | 99.6% | Above Average | $9 | Above Average | Recommended |
| Hillstone Networks SG-6000-E5960 | 99.0% | Above Average | $6 | Above Average | Recommended |
| Huawei Technologies USG6650 | 98.1% | Above Average | $7 | Above Average | Recommended |
| Juniper Networks SRX5400E | 98.0% | Above Average | $97 | Below Average | Neutral |
| Palo Alto Networks PA-7050 | 95.9% | Above Average | $31 | Below Average | Neutral |
| WatchGuard Technologies XTM 1525 | 87.7% | Below Average | $18 | Above Average | Neutral |

**Figure 2 – NSS Labs' 2016 Recommendations for Next Generation Firewall (NGFW)**

This report is part of a series of Comparative Reports on security, performance, TCO, and 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:

**Tested Products ........ 1**

**Environment ........ 1**

**Overview ........ 2**

Key Findings ........ 3

Product Rating ........ 3

**How to Read the SVM ........ 5**

*The x axis ........ 6*

*The y axis ........ 6*

**Analysis ........ 7**

Recommended ........ 7

*Check Point Software Technologies 13800 Next Generation Firewall Appliance vR77.20 ........ 7*

*Cisco FirePOWER Appliance 8350 v5.4.0.3 ........ 8*

*Dell SonicWALL SuperMassive E10800 SonicOS Enhanced v6.0.1.13-177o ........ 8*

*Forcepoint Stonesoft Next-Generation Firewall 1402 v5.8.5 ........ 9*

*Fortinet FortiGate 3200D v5.2.4, build 5069 ........ 9*

*Hillstone Networks SG-6000-E5960 v5.5 SG6000-M-2-5.5R1P2.2 ........ 10*

*Huawei Technologies USG6650 vV500R001C00SPC010T ........ 10*

Neutral ........ 11

*Barracuda Networks F600.E20 v6.1.1-071 ........ 11*

*Cisco ASA 5585-X SSP-60 v5.4.0.3 ........ 11*

*Cyberoam CR2500iNG-XP v10.6.3 ........ 12*

*Juniper Networks SRX5400E JUNOS Software Release v12.3X48 ........ 12*

*Palo Alto Networks PA-7050 v6.0.11-h1 ........ 13*

*WatchGuard Technologies XTM 1525 v11.9.4 build 486684 ........ 13*

Caution ........ 14

**Test Methodology ........ 15**

**Contact Information ........ 15**

## Table of Figures

*Figure 1 – NSS Labs 2016 Security Value Map (SVM) for Next Generation Firewall (NGFW) ........ 2*

*Figure 2 – NSS Labs' 2016 Recommendations for Next Generation Firewall (NGFW) ........ 3*

*Figure 3 – Example SVM ........ 5*

# How to Read the SVM

The SVM depicts the value of a typical deployment of ten (10) 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.

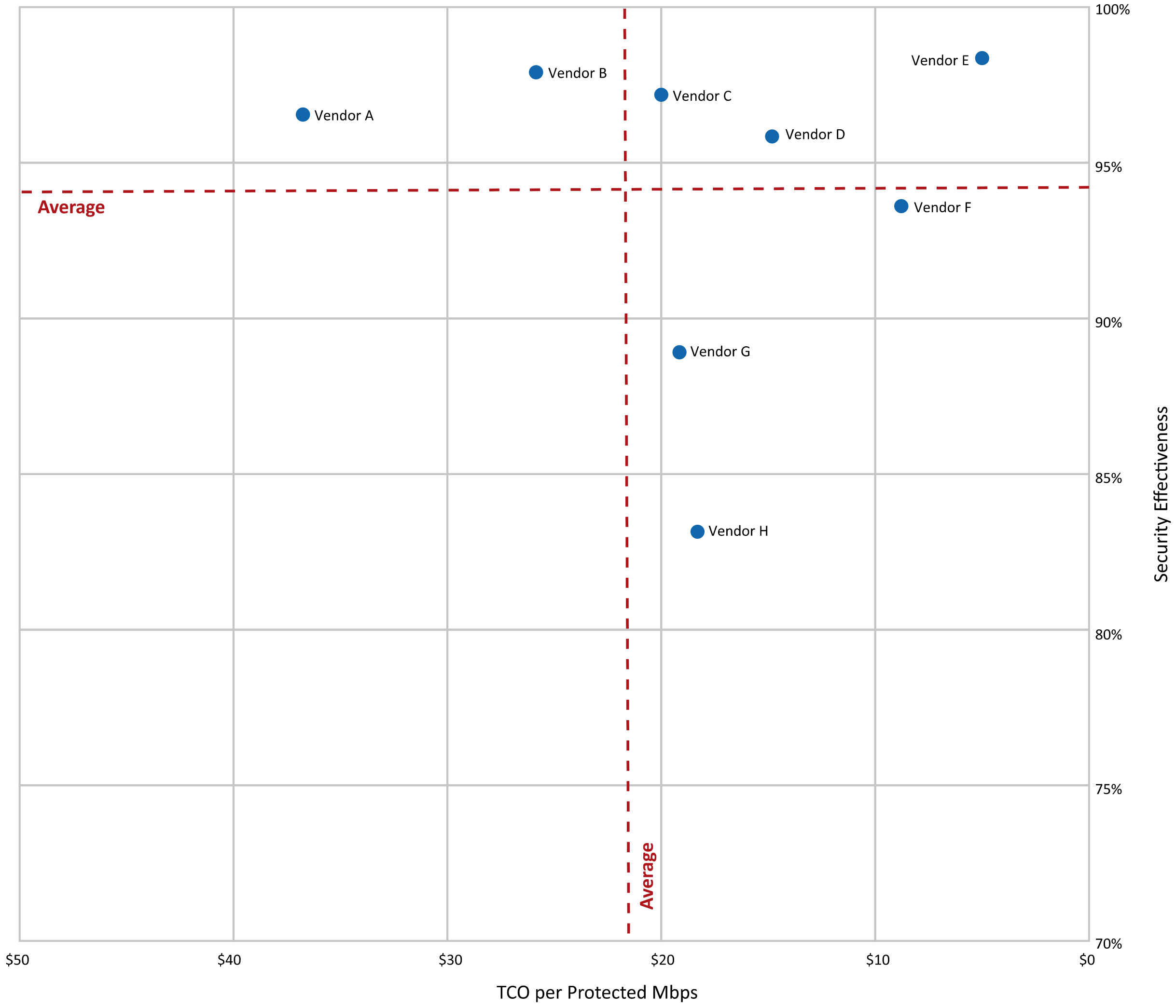

**Figure 3 – Example SVM**

No two security products deliver the same security effectiveness or performance, 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.*

**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 SVM displays two dotted lines that represent the average *Security Effectiveness* and *TCO per Protected Mbps* of all of 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.

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 13800 Next Generation Firewall Appliance vR77.20

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 100% of attacks against server applications, 99.7% of attacks against client applications, and 99.8% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 99.32% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 6,889 Mbps, which is lower than the vendor-claimed performance; Check Point rates this device at 9.5 Gbps. |

### Cisco FirePOWER Appliance 8350 v5.4.0.3

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 95.9% of attacks against server applications, 95.5% of attacks against client applications, and 95.6% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 96.94% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 17,424 Mbps, which is higher than the vendor-claimed performance; Cisco rates this device at 15 Gbps. |

### Dell SonicWALL SuperMassive E10800 SonicOS Enhanced v6.0.1.13-177o

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 95.9% of attacks against server applications, 98.7% of attacks against client applications, and 97.4% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 98.83% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 10,461 Mbps, which is lower than the vendor-claimed performance; Dell SonicWALL rates this device at 12 Gbps. |

### Forcepoint Stonesoft Next-Generation Firewall 1402 v5.8.5

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 98.8% of attacks against server applications, 98.5% of attacks against client applications, and 98.6% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 96.56% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 2,642 Mbps, which is lower than the vendor-claimed performance; Forcepoint rates this device at 4 Gbps. |

### Fortinet FortiGate 3200D v5.2.4, build 5069

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 99.6% of attacks against server applications, 99.1% of attacks against client applications, and 99.3% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 99.97% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 19,246 Mbps, which is higher than the vendor-claimed performance; Fortinet rates this device at 14 Gbps. |

### Hillstone Networks SG-6000-E5960 v5.5 SG6000-M-2-5.5R1P2.2

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 99.5% of attacks against server applications, 99.7% of attacks against client applications, and 99.6% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 98.32% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 5,570 Mbps, which is lower than the vendor-claimed performance; Hillstone rates this device at 8 Gbps. |

### Huawei Technologies USG6650 vV500R001C00SPC010T

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 97.6% of attacks against server applications, 95.3% of attacks against client applications, and 96.3% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 99.95% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 5,637 Mbps, which is lower than the vendor-claimed performance; Huawei rates this device at 8.8 Gbps. |

## Neutral

### Barracuda Networks F600.E20 v6.1.1-071

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 92.1% of attacks against server applications, 96.0% of attacks against client applications, and 94.2% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 90.53% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 2,477 Mbps, which is lower than the vendor-claimed performance; Barracuda Networks rates this device at 2.6 Gbps. |

### Cisco ASA 5585-X SSP-60 v5.4.0.3

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the Cisco ASA 5585-X SSP-60 blocked 96.5% of attacks against server applications, 95.7% of attacks against client applications, and 96.1% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 96.94% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 9,433 Mbps, which is lower than the vendor-claimed performance; Cisco rates this device at 10 Gbps. |

### Cyberoam CR2500iNG-XP v10.6.3

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 95.0% of attacks against server applications, 94.4% of attacks against client applications, and 94.7% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 98.88% of live exploits. |
| **Evasion Techniques** | The device proved effective against all evasion techniques tested. |
| **Stability and Reliability** | The device failed the following stability and reliability tests: Blocking Under Extended Attack, Passing Legitimate Traffic Under Extended Attack, State Preservation – Maximum Exceeded, and Drop Traffic – Maximum Exceeded. |
| **Firewall Policy Enforcement** | The device proved effective in enforcing all firewall policies. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 3,670 Mbps, which is lower than the vendor-claimed performance; Cyberoam rates this device at 4.5 Gbps. |

### Juniper Networks SRX5400E JUNOS Software Release v12.3X48

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 98.8% of attacks against server applications, 99.0% of attacks against client applications, and 98.9% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 97.03% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 4,138 Mbps, which is lower than the vendor-claimed performance; Juniper Networks rates this device at 22 Gbps. |

### Palo Alto Networks PA-7050 v6.0.11-h1

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 94.4% of attacks against server applications, 97.1% of attacks against client applications, and 95.8% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 95.96% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 42,324 Mbps, which is lower than the vendor-claimed performance; Palo Alto Networks rates this device at 60 Gbps. |

### WatchGuard Technologies XTM 1525 v11.9.4 build 486684

| | |
|---|---|
| ***NSS Exploit Library* Block Rate** | Using the recommended policy, the device blocked 97.4% of attacks against server applications, 99.2% of attacks against client applications, and 98.3% of attacks overall. |
| **CAWS (Live) Exploit Block Rate** | The device blocked 77.12% 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. |
| **Applications Control** | NSS engineers verified that the device successfully determined the correct application and took the appropriate action based on the policy. |
| **User/Group Identity** | For user/group identity (ID) aware policies, NSS engineers verified that the device successfully identified the users and groups and took the appropriate action based on the firewall policy. |
| **Performance Rating** | The device is rated by NSS at 2,481 Mbps, which is lower than the vendor-claimed performance; WatchGuard rates this device at 3 Gbps. |

## Caution

No vendor received a *Caution* rating in this group test.

# Test Methodology

Next Generation Firewall Test Methodology v6.0

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.