NEXT GENERATION FIREWALL COMPARATIVE ANALYSIS

Security Value Map™ (SVM)

Author – Thomas Skybakmoen

Tested Products

Barracuda F800b

Check Point 13500

Cisco ASA 5525-X

Cisco ASA 5585-X SSP60

Cisco FirePOWER 8350

Cyberoam CR2500iNG-XP

Dell SonicWALL SuperMassive E10800

Fortinet FortiGate-1500D

Fortinet FortiGate-3600C

McAfee NGF-1402

Palo Alto Networks PA-3020

WatchGuard XTM1525

Environment

Next Generation Firewall: Test Methodology v5.4

Overview

Empirical data from individual Product Analysis Reports (PARs) and Comparative Analysis Reports (CARs) is used to create the unique Security Value Map™ (SVM). The SVM illustrates the relative value of security investment options by mapping *security effectiveness* and value (*TCO per protected-Mbps*) of tested product configurations.

The SVM provides an aggregated view of the detailed findings from NSS Labs' group tests. Individual PARs are available for every product tested. CARs provide detailed comparisons across all tested products in the areas of:

- Security
- Performance
- Total cost of ownership (TCO)

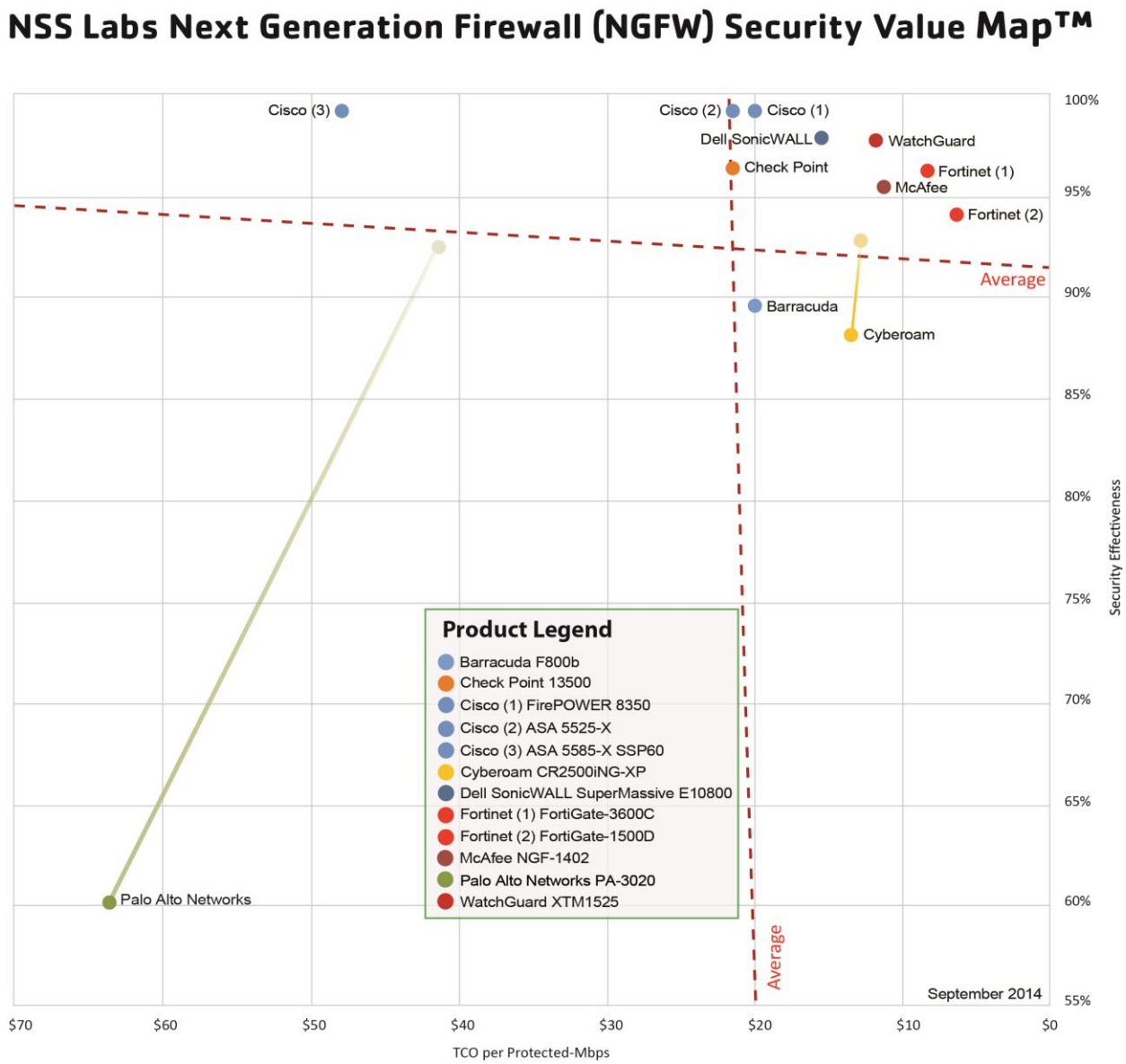

Figure 1 – NSS Labs Security Value Map (SVM) for Next Generation Firewall (NGFW)

Key Findings

- Overall *security effectiveness* varied between 60.1% and 99.2%, with 8 of the 12 tested products achieving greater than 95.0%.
- The Cyberoam CR2500iNG-XP failed one Stream Segmentation evasion test.
- The Palo Alto PA-3020 failed the RPC Fragmentation and IP Fragmentation + TCP Segmentation evasion tests.
- *TCO per protected-Mbps* varied from US$6.35 to US$63.66, with most tested devices costing below US$25.00 *per protected-Mbps*.
- *NSS-tested throughput* ranged from 719 Mbps to 18,771 Mbps.
- Average *security effectiveness* rating was 91.5% – 9 devices were rated as above average *security effectiveness*, 3 were rated as below average.
- Average *value* (*TCO per protected-Mbps*) was US$21.80 – 10 devices were rated as above average *value* and two were below average.

Product Rating

The *Overall Rating* in figure 2 is determined based on which SVM quadrant 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, please see the *"How to Read the SVM"* section in this document.

Product	Security Effectiveness		Value (TCO Per Protected-Mbps)		Overall Rating
Barracuda F800b	89.70%	Below Average	$20.03	Above Average	Neutral
Check Point 13500	96.40%	Above Average	$21.45	Above Average	Recommended
Cisco ASA 5525-X	99.20%	Above Average	$21.60	Above Average	Recommended
Cisco ASA 5585-X SSP60	99.20%	Above Average	$48.00	Below Average	Neutral
Cisco FirePOWER 8350	99.20%	Above Average	$20.03	Above Average	Recommended
Cyberoam CR2500iNG-XP	88.20%	Below Average	$13.48	Above Average	Neutral
Dell SonicWALL SuperMassive E10800	97.90%	Above Average	$15.46	Above Average	Recommended
Fortinet FortiGate-1500D	94.10%	Above Average	$6.35	Above Average	Recommended
Fortinet FortiGate-3600C	96.30%	Above Average	$8.30	Above Average	Recommended
McAfee NGF-1402	95.50%	Above Average	$11.38	Above Average	Recommended
Palo Alto Networks PA-3020	60.10%	Below Average	$63.66	Below Average	Caution
WatchGuard XTM1525	97.80%	Above Average	$11.87	Above Average	Recommended

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

This report is part of a series of CARs 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, please visit http://www.nsslabs.com.

Table of Contents:

Table of Figures

How to Read the SVM

The SVM depicts the value of a typical deployment of twenty (20) devices plus one (1) central management unit (and where necessary, a log aggregation, and/or event management unit), to provide a more accurate reflection of cost than if only a single NGFW device were depicted. An example SVM is shown in figure 3.

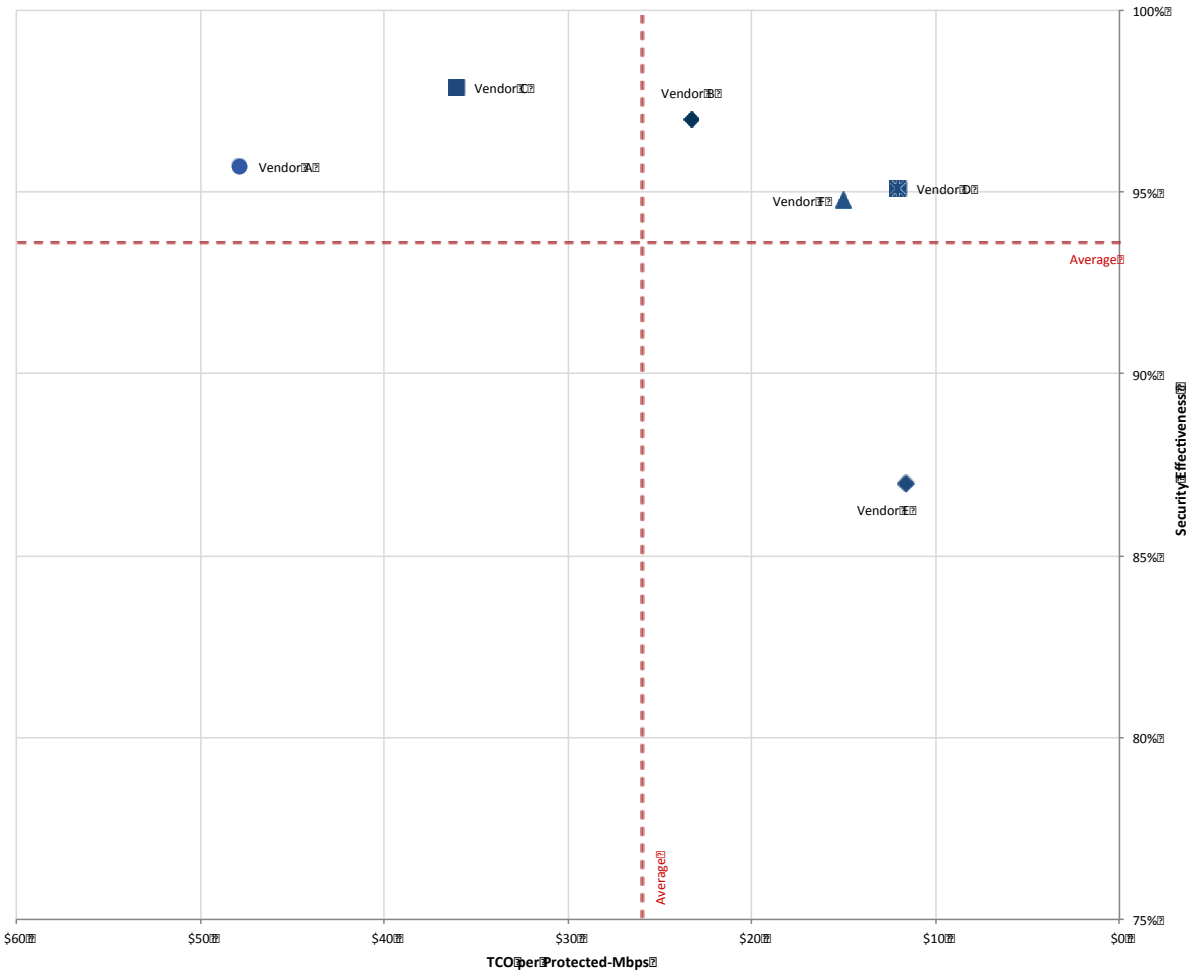

Figure 3 – Example SVM

The x-axis charts the *TCO per protected-Mbps*, a metric that incorporates the 3-Year TCO with the *NSS-tested throughput* to provide a data point by which to compare the actual value of each product tested. The terms *TCO per protected-Mbps* and *value* are used interchangeably throughout the CARs.

The y-axis charts the *security effectiveness* as determined in the *security effectiveness* tests. Devices that are missing critical security capabilities will have a reduced score on this axis.

Mapping the data points against the *security effectiveness* and *TCO per protected-Mbps* results in four quadrants on the SVM.

- **Products that map farther up and to the right are recommended.** The upper-right quadrant contains those products that are in the ***Recommended*** category for both *security effectiveness* and *TCO per protected-Mbps.* These products provide a high level of detection and value for money.
- **Products that map farther down and to the left should be used with caution**. The lower left quadrant would comprise the ***Caution*** category; these products offer limited value for money given the 3-year TCO and measured *security effectiveness* rating.
- The remaining two quadrants comprise the ***Neutral*** category. Products that fall into this category may still be worthy of a place on an organization's short list based on its specific requirements.

For example, products in the upper-left quadrant score as *above average* for *security effectiveness*, but below average for *value* (*TCO per protected-Mbps)*. These products would be suitable for environments requiring a high level of detection, albeit at a higher than average cost.

Conversely, products in the lower-right quadrant score as below average for *security effectiveness*, but above average for *value* (*TCO per protected-Mbps)*. These products would be suitable for environments where budget is paramount, and 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 completely customized SVM. Furthermore, the option is available to schedule an inquiry with NSS analysts.

Analysis

Analysis is divided into three categories based on the position of each product in the SVM: ***Recommended***, ***Neutral***, and ***Caution***. Each of the tested products will fall into only one category, and vendors are listed alphabetically within each section.

Recommended

Check Point 13500

Key Findings:

- Using the recommended policy, the Check Point 13500 NGFW blocked 97.1% of attacks against server applications, 95.9% of attacks against client applications, and 96.4% overall.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The 13500 NGFW proved effective in enforcing all firewall policies.
- For applications control, testing verified that the 13500 NGFW correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- For user/group identity (ID) aware policies, testing verified that the 13500 NGFW correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- The 13500 NGFW is rated by NSS at 6,699 Mbps, which is higher than the vendor-claimed performance (Check Point Software Technologies rates this device at 5.7 Gbps).

Cisco ASA 5525-X

Key Findings:

- Using the recommended policy, the Cisco ASA 5525-X blocked 99.5% of attacks against server applications, 99.0% of attacks against client applications, and 99.2% overall.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The ASA 5525-X proved effective in enforcing all firewall policies.
- For applications control, testing verified that the ASA 5525-X correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- For user/group identity (ID) aware policies, testing verified that the ASA 5525-X correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- The ASA 5525-X is rated by NSS at 954 Mbps, which exceeds the vendor-claimed performance (Cisco rates this device at 650 Mbps).

Cisco FirePOWER 8350

Key Findings:

- Using the recommended policy, the Cisco FirePOWER 8350 blocked 99.5% of attacks against server applications, 99.0% of attacks against client applications, and 99.2% overall.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The FirePOWER 8350 proved effective in enforcing all firewall policies.
- For applications control, testing verified that the FirePOWER 8350 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- For user/group identity (ID) aware policies, testing verified that the FirePOWER 8350 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- The FirePOWER 8350 is rated by NSS at 18,771 Mbps, which exceeds the vendor-claimed performance (Cisco rates this device at 15 Gbps).

Dell SonicWALL SuperMassive E10800

Key Findings:

- Using the recommended policy, the Dell SonicWALL SuperMassive E10800 blocked 96.4% of attacks against server applications, 99.1% of attacks against client applications, and 97.9% overall.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The E10800 proved effective in enforcing all firewall policies.
- For applications control, testing verified that the E10800 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- For user/group identity (ID) aware policies, testing verified that the E10800 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications. While the E10800 offers Active Directory integration, it was not configured for use in testing. The E10800 local firewall database integration implementation was used.
- The E10800 is rated by NSS at 16,395 Mbps, which is higher than the vendor-claimed performance (Dell SonicWALL rates this device at 12 Gbps).

Fortinet FortiGate-1500D

Key Findings:

- Using the recommended policy, the Fortinet FortiGate-1500D blocked 97.0% of attacks against server applications, 91.8% of attacks against client applications, and 94.1% overall.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The FortiGate-1500D proved effective in enforcing all firewall policies.
- For applications control, testing verified that the FortiGate-1500D correctly enforced complex outbound and inbound policies consisting of multiple rules, objects, and applications.
- For user/group identity (ID) aware policies, testing verified that the FortiGate-1500D correctly enforced complex outbound and inbound policies consisting of multiple rules, objects, and applications.
- The FortiGate-1500D is rated by NSS at 9,597 Mbps, which is lower than the vendor-claimed performance (Fortinet rates this device at 11,000 Mbps).

Fortinet FortiGate-3600C

Key Findings:

- Using the recommended policy, the Fortinet FortiGate-3600C blocked 98.3% of attacks against server applications, 94.7% of attacks against client applications, and 96.3% overall.
- The device proved effective against all evasion techniques tested.
- The device also passed all of the stability and reliability tests.
- The FortiGate-3600C proved effective in enforcing all firewall policies.
- For applications control, testing found that the FortiGate-3600C correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- For user/group identity (ID) aware policies, testing verified that the FortiGate-3600C correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- The FortiGate-3600C is rated by NSS at 17,050 Mbps, which is higher than the vendor-claimed performance (Fortinet rates this device at 14,000 Mbps).

McAfee NGF-1402

Key Findings:

- Using the recommended policy, the McAfee NGF-1402 blocked 96.6% of attacks against server applications, 94.6% of attacks against client applications, and 95.5% overall.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The NGF-1402 proved effective in enforcing all firewall policies.
- For applications control, testing found that the NGF-1402 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- For user/group identity (ID) aware policies, testing verified that the NGF-1402 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- The NGF-1402 is rated by NSS at 5,086 Mbps, which is higher than the vendor-claimed performance (McAfee rates this device at 4.5 Gbps).

WatchGuard XTM1525

Key Findings:

- Using the recommended policy, the WatchGuard Technologies Inc. XTM1525 blocked 96.7% of attacks against server applications, 98.7% of attacks against client applications, and 97.8% overall.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The XTM1525 proved effective in enforcing all firewall policies.
- For applications control, testing found that the XTM1525 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- For user/group identity (ID) aware policies, testing verified that XTM1525 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications. While the XTM1525 offers Active Directory integration, it was not configured for use in testing. The XTM1525 local firewall database integration implementation was used.
- The XTM1525 is rated by NSS at 3,363 Mbps, which is lower than the vendor-claimed performance (WatchGuard Technologies Inc. rates this device at 13 Gbps).

Neutral

Barracuda F800b

Key Findings:

- Using the recommended policy, the Barracuda NG FIREWALL F800b blocked 89.1% of attacks against server applications, 90.1% of attacks against client applications, and 89.7% overall.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The NG FIREWALL F800b proved effective in enforcing all firewall policies.
- For applications control, testing found that the NG FIREWALL F800b correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- For user/group identity (ID) aware policies, testing verified that the NG FIREWALL F800b correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- The NG FIREWALL F800b is rated by NSS at 1,636 Mbps, which is lower than the vendor-claimed performance (Barracuda Networks rates this device at 1.8 Gbps).

Cisco ASA 5585-X SSP60

Key Findings:

- Using the recommended policy, the Cisco ASA 5585-X SSP60 blocked 99.5% of attacks against server applications, 99.0% of attacks against client applications, and 99.2% overall.
- The device proved effective against all evasion techniques tested.
- The device also passed stability and reliability tests.
- The ASA 5585-X SSP60 proved effective in enforcing all firewall policies.
- For applications control, testing found that the ASA 5585-X SSP60 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- For user/group identity (ID) aware policies, testing verified that the ASA 5585-X SSP60 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- The ASA 5585-X SSP60 is rated by NSS at 9,500 Mbps, which exceeds the vendor-claimed performance (Cisco rates this device at 6,000 Mbps).

Cyberoam CR2500iNG-XP

Key Findings:

- Using the recommended policy, the Cyberoam Technologies Pvt. Ltd CR2500iNG-XP blocked 94.6% of attacks against server applications, 91.4% of attacks against client applications, and 92.8% overall.
- The device failed to protect against Stream Segmentation.
- The device also passed all stability and reliability tests.
- The CR2500iNG-XP proved effective in enforcing all firewall policies.
- For applications control, testing found that the CR2500iNG-XP correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- For user/group identity (ID) aware policies, testing verified that the CR2500iNG-XP correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications. While the CR2500iNG-XP offers Active Directory integration, it was not configured for use in testing. The CR2500iNG-XP local firewall database integration implementation was used.
- The CR2500iNG-XP is rated by NSS at 4,019 Mbps, which is lower than the vendor-claimed performance (Cyberoam Technologies Pvt. Ltd. rates this device at 8 Gbps).

Caution

Palo Alto Networks PA-3020

Key Findings:

- Using the recommended policy, the Palo Alto Networks PA-3020 blocked 93.1% of attacks against server applications, 92.0% of attacks against client applications, and 92.5% overall.
- The device failed to protect against the following evasion techniques: RPC Fragmentation and IP Fragmentation + TCP Segmentation.
- The device passed all stability and reliability tests.
- The PA-3020 proved effective in enforcing all firewall policies.
- For applications control, testing found that the PA-3020 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- For user/group identity (ID) aware policies, testing verified that the PA-3020 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications.
- The PA-3020 is rated by NSS at 719 Mbps, which is lower than the vendor-claimed performance (Palo Alto Networks rates this device at 1 Gbps).

Test Methodology

Next Generation Firewall: v5.4

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 Rd
Buliding A, Suite 200
Austin, TX 78746
info@nsslabs.com
www.nsslabs.com

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

© 2014 NSS Labs, Inc. All rights reserved. No part of this publication may be reproduced, copied/scanned, stored on a retrieval system, e-mailed or otherwise disseminated or transmitted without the express written consent of NSS Labs, Inc. ("us" or "we").

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.