



NEXT GENERATION FIREWALL COMPARATIVE REPORT

Security

JULY 17, 2019

Author – Thomas Skybakmoen

Tested Products

Barracuda Networks CloudGen Firewall F800.CCE v7.2.3

Check Point Software Technologies 6500 Security Gateway R80.20

Forcepoint 2105 NGFW v6.3.11

Fortinet FortiGate 500E v6.0.4 build 0231

Huawei USG6620E v600R006C00SPC310

Palo Alto Networks PA-5220 PAN-OS 8.1.6-h2

Sophos XG 750 Firewall SFOS v17.5

SonicWall NS 4650 SonicOS v6.5

Versa Networks FlexVNF v16.1R2-S7

WatchGuard Firebox M670 Firmware: 12.3 B589695 Ver-4.907

Vendor A

Vendor B

Environment

NSS Labs Next Generation Firewall Test Methodology v9.0

NSS Labs SSL/TLS Performance Test Methodology v1.3

NSS Labs Evasions Test Methodology v1.1

Overview

Implementation of next generation firewall (NGFW) devices can be a complex process with multiple factors affecting overall security effectiveness. The following factors should be considered over the course of the useful life of the device:

- Deployment use cases:
 - Will the NGFW be deployed to protect servers or desktop clients, or both?
 - How old are the operating systems and applications?
- Defensive capabilities in the deployment use cases (exploit block rate)
- Anti-evasion capabilities (resistance to common evasion techniques)
- Device stability and reliability

In order to determine the relative security effectiveness of devices on the market and to facilitate accurate product comparisons, NSS Labs has developed a unique metric:

$$\text{Security Effectiveness} = \text{Exploit Block Rate}^1 * \text{Evasions} * \text{Stability and Reliability}$$

Figure 1 – Security Effectiveness Formula

By focusing on security effectiveness as a whole instead of on exploit block rate alone, NSS is able to factor in the ease with which defenses can be bypassed, as well as the reliability of the device. Figure 2 presents the overall results of the tests.

Vendor	Block Rate	Evasions	Stability and Reliability	Security Effectiveness
Barracuda Networks	92.7%	99%	100%	91.7%
Check Point Software Technologies	98.4%	99%	100%	97.4%
Forcepoint	97.2%	99%	100%	96.2%
Fortinet	99.0%	94%	100%	93.0%
Huawei	96.2%	98%	100%	94.2%
Palo Alto Networks	97.9%	100%	100%	97.9%
SonicWall	97.6%	97%	100%	94.7%
Sophos	94.2%	99%	100%	93.3%
Versa Networks	99.0%	94%	100%	93.1%
WatchGuard	96.5%	100%	100%	96.5%
Vendor A	98.3%	79%	100%	77.7%
Vendor B	88.4%	93%	100%	82.2%

Figure 2 – Security Effectiveness

¹Exploit block rate is defined as the total number of samples (live exploits and exploits from the *NSS Labs Exploit Library*) that are blocked under test.

NSS research indicates that NGFWs are typically deployed to protect users rather than data center assets and that the majority of enterprises will not separately tune intrusion prevention system (IPS) modules within their NGFWs. Therefore, during NSS testing, NGFW products are configured with the vendor’s pre-defined or recommended (i.e., “out-of-the-box”) settings in order to provide readers with relevant security effectiveness and performance dimensions based on their expected usage.

The comprehensive *NSS Labs Exploit Library* covers a diverse set of exploits focused on several hundred applications and operating systems. Protection from web-based exploits (live attacks) that are currently targeting client applications can be effectively measured using NSS’ cloud platform for continuous security validation. Figure 3 depicts how each product scored against live exploits and exploits from the *NSS Labs Exploit Library*. For details on each product’s block rate, please see the sections on Live Exploits and NSS Labs Exploit Library.

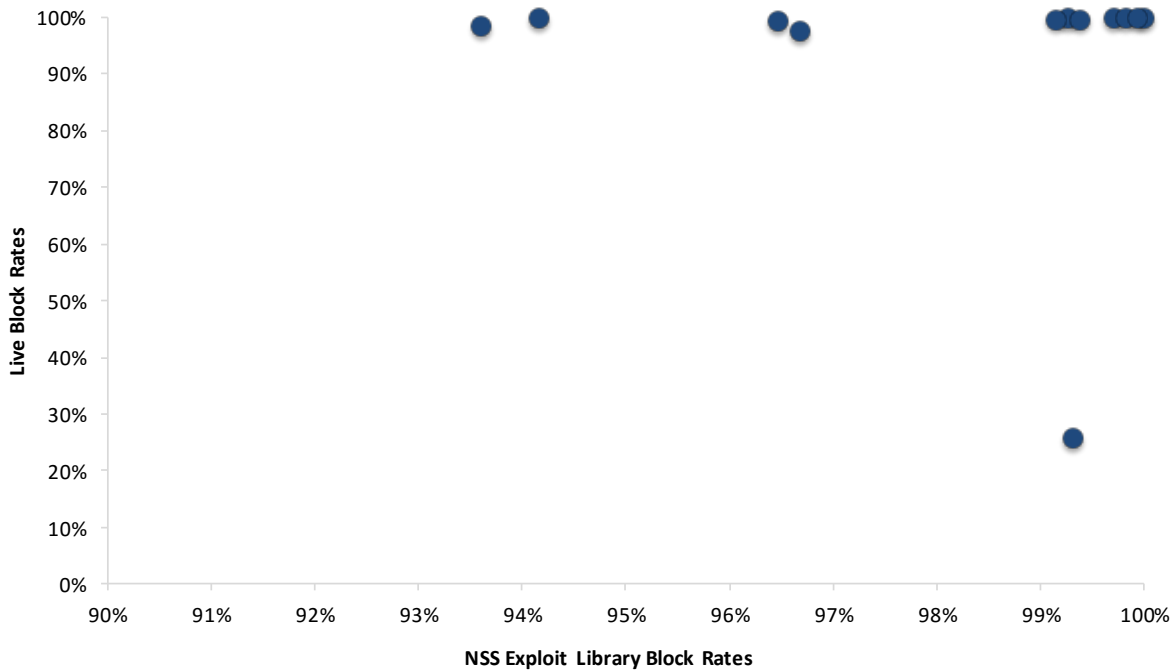


Figure 3 – Protection Against Live Exploits and Exploits from the *NSS Labs Exploit Library*

Table of Contents

Tested Products	1
Environment	1
Overview	2
Analysis	5
Live Exploits.....	5
NSS Labs Exploit Library.....	6
Coverage by Date	6
Coverage by Attack Vector	7
Coverage by Impact Type	9
Resistance to Evasion Techniques	9
Stability and Reliability	11
Security Effectiveness	12
Test Methodology	13
Contact Information	13

Table of Figures

Figure 1 – Security Effectiveness Formula	2
Figure 2 – Security Effectiveness	2
Figure 3 – Protection Against Live Exploits and Exploits from the <i>NSS Labs Exploit Library</i>	3
Figure 4 – Live Exploits.....	6
Figure 5 – Coverage by Date	7
Figure 6 – Attacker-Initiated Exploit Block Rate (Server Side)	8
Figure 7 – Target-Initiated Exploit Block Rate (Client Side)	8
Figure 8 – Overall Exploit Block Rate	8
Figure 9 – Evasion Resistance	10
Figure 10 – Stability and Reliability	11
Figure 11 – Security Effectiveness	12

Analysis

The firewall market is one of the largest and most mature security markets. Firewalls have undergone several stages of development, from early packet filtering and circuit relay firewalls to application-layer (proxy-based) and dynamic packet filtering firewalls. Throughout their history, however, the goal has been to enforce an access control policy between two networks, and they should therefore be viewed as an implementation of policy.

A firewall is a mechanism used to protect a trusted network from an untrusted network, while allowing authorized communications to pass from one side to the other, thus facilitating secure business use of the Internet. With the emergence of HTML 5, web browsers, and security threats, however, firewalls are evolving further. NGFWs traditionally have been deployed to defend the network on the edge, but some enterprises have expanded their deployment to include internal segmentation.

As Web 3.0 trends push critical business applications through firewall ports that previously were reserved for a single function, such as HTTP, legacy firewall technology is effectively blinded. It is unable to differentiate between actual HTTP traffic and non-HTTP services tunneling over port 80, such as VoIP or instant messaging. Today, application-level monitoring must be performed in addition to analysis of port and destination. Firewalls are evolving to address this increased complexity.

It is no longer possible to rely on port and protocol combinations alone to define network applications. The NGFW must be capable of determining which applications are running regardless of which ports they are using, in order to secure them effectively. This section verifies that the device is capable of enforcing the security policy effectively.

Live Exploits

This test used NSS' continuous live testing capabilities to determine how effective products are at blocking exploits that are being used, or that have been used in active attack campaigns.²

Protection from web-based exploits targeting client applications, also known as “drive-by” downloads, can be effectively measured in NSS' unique live test harness through a series of procedures that measure the stages of protection.

Unlike traditional malware that is downloaded and installed, “drive-by” attacks first exploit a vulnerable application then silently download and install malware.

² See the NSS Continuous Security Validation Platform for more details.

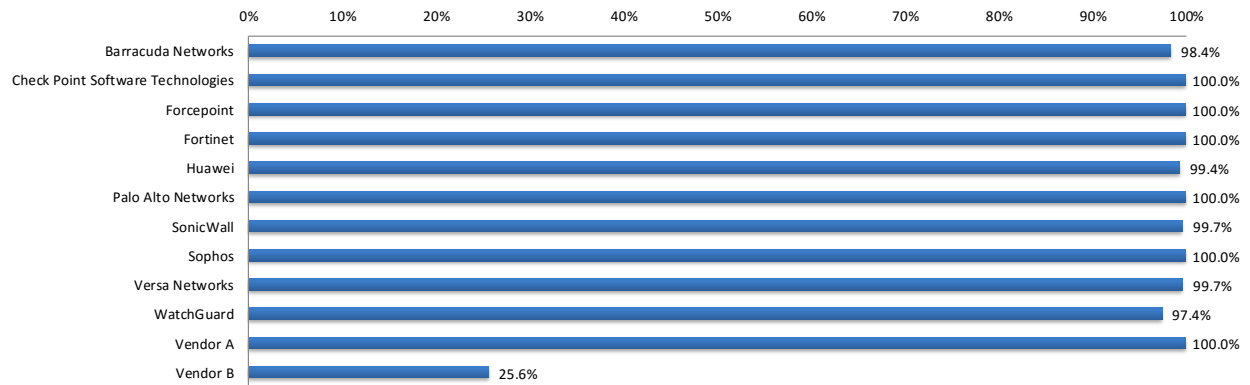


Figure 4 – Live Exploits

NSS Labs Exploit Library

NSS’ security effectiveness testing leverages the deep expertise of our engineers who utilize multiple commercial, open-source, and proprietary tools as appropriate. With more than 1,700 exploits, this is the industry’s most comprehensive test to date.

Coverage by Date

Contrary to popular belief, the biggest risks are not always driven by the latest “Patch Tuesday” disclosures. NSS’ threat research reveals that many older attacks are still in circulation and therefore remain relevant.

Different vendors take different approaches to adding coverage once a vulnerability is disclosed. Attempts to provide rapid coverage for vulnerabilities that are not fully understood can result in multiple exploit-specific signatures that may be inaccurate, ineffective, or prone to false positives. Vendors that have the resources to fully research a vulnerability should be able to produce vulnerability-oriented signatures that provide coverage for all exploits written to take advantage of that flaw. This approach provides more effective coverage with fewer false positives.

Vendors may retire older signatures in an attempt to alleviate a product’s performance limitations; however, this may result in inconsistent coverage for older vulnerabilities and varying levels of protection across products.

Figure 5 classifies coverage according to disclosure date, as tracked by CVE numbers. The heat map displays vendor coverage by year (dark green = high coverage; dark red = low coverage).

Product/Year	Barracuda Networks	Check Point	Forcepoint	Fortinet	Huawei	Palo Alto Networks	SonicWall	Sophos	Versa Networks	WatchGuard	Vendor A	Vendor B
2008	94.0%	100.0%	100.0%	99.7%	99.1%	100.0%	99.4%	96.8%	100.0%	98.4%	100.0%	99.1%
2009	93.0%	98.9%	100.0%	100.0%	97.3%	100.0%	98.9%	98.9%	99.5%	97.3%	99.5%	99.5%
2010	90.5%	100.0%	100.0%	100.0%	93.9%	100.0%	98.8%	90.5%	98.5%	96.3%	99.7%	99.4%
2011	90.7%	99.2%	100.0%	100.0%	84.7%	100.0%	100.0%	80.5%	98.3%	96.6%	99.2%	100.0%
2012	94.1%	99.5%	100.0%	100.0%	93.1%	100.0%	99.5%	89.7%	100.0%	99.0%	100.0%	99.0%
2013	100.0%	100.0%	100.0%	100.0%	98.8%	100.0%	100.0%	89.2%	100.0%	100.0%	100.0%	100.0%
2014	98.9%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	97.8%	100.0%	100.0%
2015	87.5%	100.0%	100.0%	99.0%	100.0%	100.0%	99.0%	97.9%	100.0%	96.9%	99.0%	97.9%
2016	97.1%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	99.6%	98.9%	94.2%	98.9%	99.6%
2017	91.1%	100.0%	100.0%	98.2%	96.4%	100.0%	100.0%	98.2%	98.2%	87.5%	94.6%	100.0%
2018	94.6%	97.3%	100.0%	100.0%	100.0%	97.3%	97.2%	88.9%	91.9%	91.7%	91.9%	97.2%
TOTAL	93.6%	99.7%	100.0%	99.8%	96.5%	99.9%	99.4%	94.2%	99.2%	96.7%	99.3%	99.3%

Figure 5 – Coverage by Date

Coverage by Attack Vector

Exploits can be initiated against a server either locally by the target (desktop client) or remotely by the attacker. Since 2007, NSS researchers have noticed a dramatic rise in the number of client-side exploits, as these can be easily launched by unsuspecting users who visit infected websites. At first, IPS products did not focus on these types of attacks as they were considered the responsibility of antivirus products.

This approach is no longer viewed as acceptable and, despite the difficulty of providing extensive coverage for client-side attacks, the IPS (and NGFW) industry has attempted to provide more complete coverage of these attacks. This is particularly important for NGFW devices, which are typically used to protect client desktops rather than data centers and servers; the latter comprise deployment scenarios where separate dedicated firewall and IPS devices are more common.

Attacks can be categorized as either attacker initiated or target initiated.

- Attacker-initiated attacks are executed remotely by the attacker against a vulnerable application and/or operating system. These attacks traditionally target servers (which is why they are often referred to as server-side attacks).
- Target-initiated attacks are initiated by the vulnerable target (which is why they are often referred to as client-side attacks). The attacker has little or no control over when the target user or application will execute the threat. Target examples include Internet Explorer, Adobe Reader, Mozilla Firefox, QuickTime, and Microsoft Office applications.

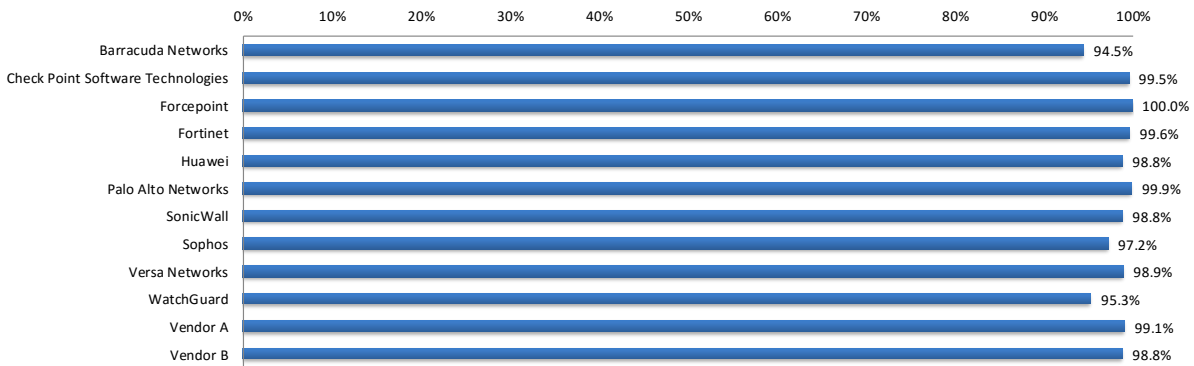


Figure 6 – Attacker-Initiated Exploit Block Rate (Server Side)

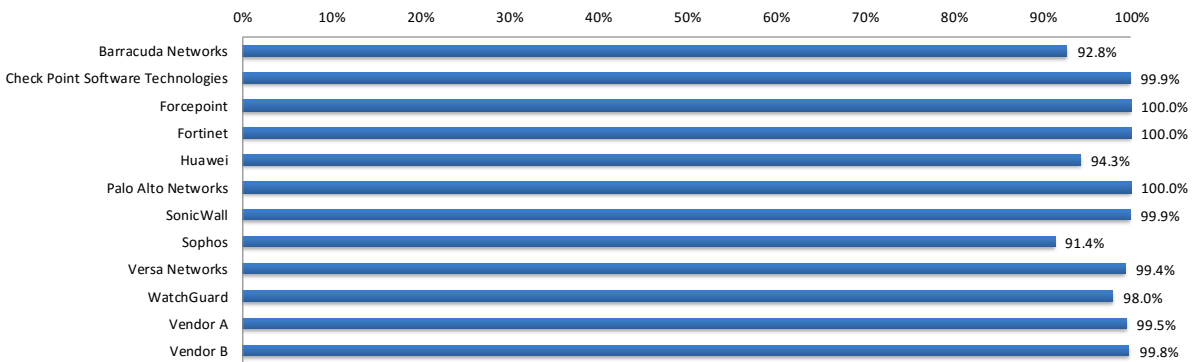


Figure 7 – Target-Initiated Exploit Block Rate (Client Side)

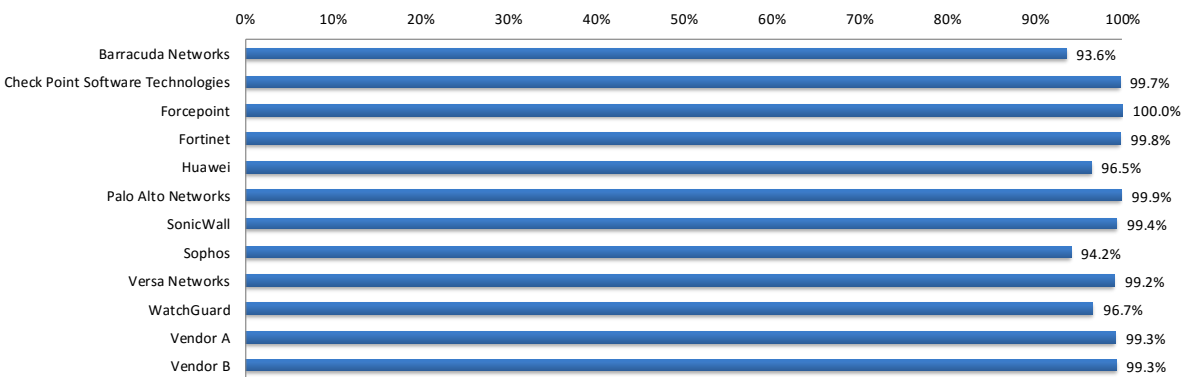


Figure 8 – Overall Exploit Block Rate

NSS research indicates that most enterprises are forced to support a heterogeneous mix of desktop client applications. Further, enterprise IT departments are often unable to positively identify which client applications are running on their employees’ desktops, and which are not.

This research provides new clarity regarding tuning best practices and indicates that it is still necessary to tune an NGFW that is protecting servers in a DMZ or data center. Research also indicates that with regard to protecting desktop client applications with an NGFW, it is often best to enable a (nearly) full complement of signatures, since it is not feasible to tune an NGFW based on specific desktop client applications.

Coverage by Impact Type

The most serious exploits are those that result in a remote system compromise, providing the attacker with the ability to execute arbitrary system-level commands. Most exploits in this class are “weaponized” and offer the attacker a fully interactive remote shell on the target client or server.

Slightly less serious are attacks that result in an individual service compromise, but not arbitrary system-level command execution. Finally, there are attacks that result in a system- or service-level fault that crashes the targeted service or application and requires administrative action to restart the service or reboot the system. Clients can contact NSS for more information about these tests.

Resistance to Evasion Techniques

Evasion techniques are a means of disguising and modifying attacks at the point of delivery to avoid detection and blocking by security products. Failure of a security device to correctly identify a specific type of evasion potentially allows an attacker to use an entire class of exploits for which the device is assumed to have protection. This often renders the device virtually useless. Many of the techniques used in this test have been widely known for years and should be considered minimum requirements for the NGFW product category.

Providing exploit protection results without fully factoring in evasions can be misleading. The more classes of evasion that are missed (such as HTTP evasions, IP packet fragmentation, TCP stream segmentation, RPC fragmentation, URL obfuscation, HTML obfuscation, resiliency, and FTP evasion), the less effective the device. For example, it is better to miss all techniques in one evasion category, such as FTP evasion, than one technique in each category, which would result in a broader attack surface.

Furthermore, evasions operating at the lower layers of the network stack (IP packet fragmentation or stream segmentation) have a greater impact on security effectiveness than those operating at the upper layers (HTTP or FTP obfuscation). Lower-level evasions will potentially impact a wider number of exploits; missing TCP segmentation, for example, is a much more serious issue than missing FTP obfuscation.

The resiliency of a system can be defined as its ability to absorb an attack and reorganize around a threat. When an attacker is presented with a vulnerability, the attacker can select one or more paths to trigger the vulnerability. NSS introduced various previously unseen variations of exploits to exploit the vulnerability and measure a device’s effectiveness against them. A resilient device can detect and prevent against different variations of an exploit. For more, see the Evasions Test Methodology v1.1 at www.nsslabs.com.

Figure 9 provides evasion resistance results for each the tested products. For additional details on which evasions were missed, see the individual Test Reports.

Evasion Type	Barracuda Networks	Check Point	Forcepoint	Fortinet	Huawei	Palo Alto Networks	SonicWall	Sophos	Versa Networks	WatchGuard	Vendor A	Vendor B
IP Packet Fragmentation/ TCP Segmentation	PASS	PASS	PASS	FAIL	FAIL	PASS	FAIL	PASS	FAIL	PASS	FAIL	FAIL
RPC Fragmentation	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
URL Obfuscation	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
FTP/Telnet Evasion	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
HTTP Evasions	PASS	PASS	FAIL	PASS	PASS	PASS	PASS	PASS	PASS	PASS	FAIL	PASS
HTTP Evasions over SSL/TLS ³	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	FAIL	PASS
HTML Evasions	PASS	FAIL	PASS	FAIL	FAIL	PASS	FAIL	PASS	PASS	PASS	FAIL	FAIL
Script Obfuscations	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Attacks on Nonstandard Ports	PASS	PASS	PASS	PASS	PASS	PASS	PASS	FAIL	PASS	PASS	FAIL	PASS
Combination of Evasions	FAIL	PASS	PASS	PASS	PASS	PASS	FAIL	FAIL	FAIL	PASS	FAIL	FAIL

Figure 9 – Evasion Resistance

³ The evasion techniques used in the HTTPS test are the same techniques used in the HTTP test. The device was expected to decrypt, inspect, and then re-encrypt traffic.

Stability and Reliability

Long-term stability is particularly important for an inline device, where failure can produce a network outage. These tests verify the device’s ability to block malicious traffic while under extended load. Products that cannot sustain legitimate traffic while under test will fail.

The device is required to remain operational and stable throughout all these tests, and to block 100% of previously known malicious attacks, raising an alert for each. If any non-allowed traffic passes successfully, caused either by the volume of traffic or by the device failing open for any reason, it will fail the test. All products passed the stability and reliability tests. For additional details, please see the individual Test Reports.

Vendor	Stability and Reliability
Barracuda Networks	PASS
Check Point Software Technologies	PASS
Forcepoint	PASS
Fortinet	PASS
Huawei	PASS
Palo Alto Networks	PASS
SonicWall	PASS
Sophos	PASS
Versa Networks	PASS
WatchGuard	PASS
Vendor A	PASS
Vendor B	PASS

Figure 10 – Stability and Reliability

Security Effectiveness

The overall security effectiveness of an NGFW is determined using the formula in Figure 1. NSS combines a product's scores relating to block rate, evasions, and stability and reliability in order to generate an overall *Security Effectiveness* score for the device.

Vendor	Block Rate	Evasions	Stability and Reliability	Security Effectiveness
Barracuda Networks	92.7%	99%	100%	91.7%
Check Point Software Technologies	98.4%	99%	100%	97.4%
Forcepoint	97.2%	99%	100%	96.2%
Fortinet	99.0%	94%	100%	93.0%
Huawei	96.2%	98%	100%	94.2%
Palo Alto Networks	97.9%	100%	100%	97.9%
SonicWall	97.6%	97%	100%	94.7%
Sophos	94.2%	99%	100%	93.3%
Versa Networks	99.0%	94%	100%	93.1%
WatchGuard	96.5%	100%	100%	96.5%
Vendor A	98.3%	79%	100%	77.7%
Vendor B	88.4%	93%	100%	82.2%

Figure 11 – Security Effectiveness

Test Methodology

NSS Labs Next Generation Firewall Test Methodology v9.0

NSS Labs SSL/TLS Performance Test Methodology v1.3

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

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

© 2019 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.