NEXT GENERATION FIREWALL COMPARATIVE REPORT

Security

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

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

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:

***Security Effectiveness** = Exploit Block Rate[1] * Evasions* 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	95.4%	100%	100%	95.4%
Check Point	99.2%	96%	25%	25.0%
Cisco	95.7%	75%	100%	71.8%
Forcepoint	99.7%	100%	100%	99.7%
Fortinet	99.3%	100%	100%	99.3%
Palo Alto Networks	98.7%	100%	100%	98.7%
SonicWall	98.8%	100%	100%	98.8%
Sophos	93.5%	25%	100%	25.0%
Versa Networks	90.4%	100%	100%	90.4%
WatchGuard	97.2%	92%	100%	89.1%

Figure 2 – Security Effectiveness

[1]Exploit block rate is defined as the total number of samples (live exploits and exploits from NSS 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 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 the NSS Labs cloud platform for continuous security validation. Figure 3 depicts how each vendor scored against live exploits and the *NSS Exploit Library*. For details on block rate, please see the Live Exploits and NSS Exploit Library chapters.

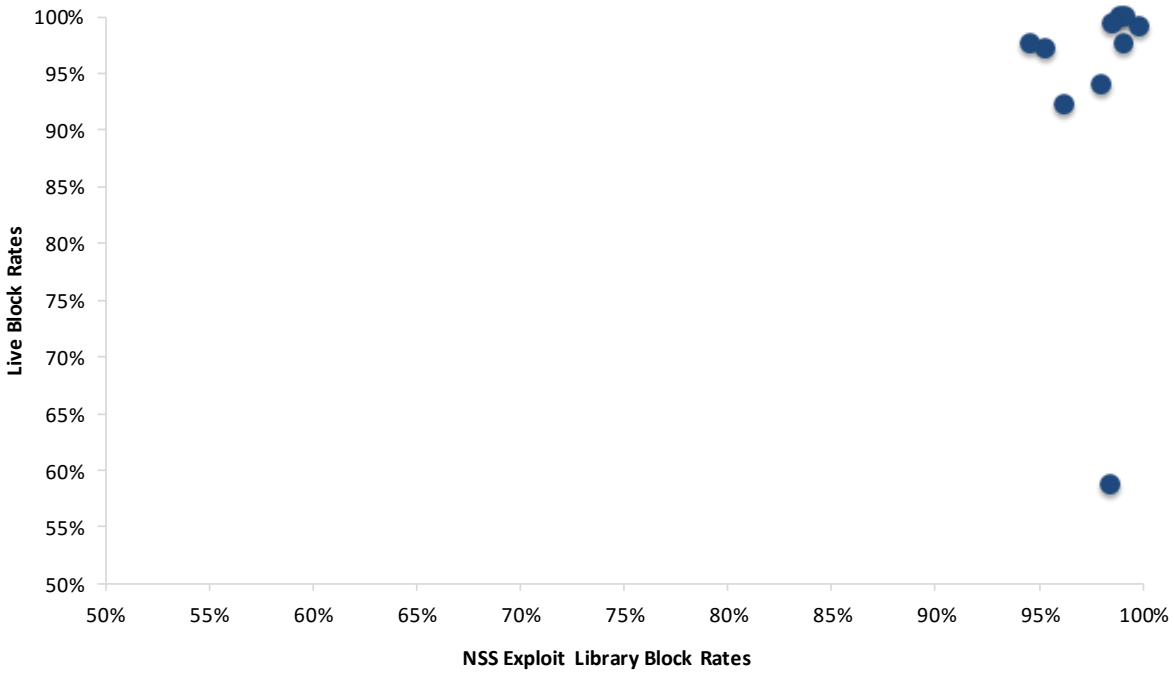

Figure 3 – Protection Against Live Exploits and Exploits from the *NSS Exploit Library*

Table of Contents

Table of Figures

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 and thus secure them effectively. This section verifies that the device is capable of enforcing the security policy effectively.

Live Exploits

This test uses 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.

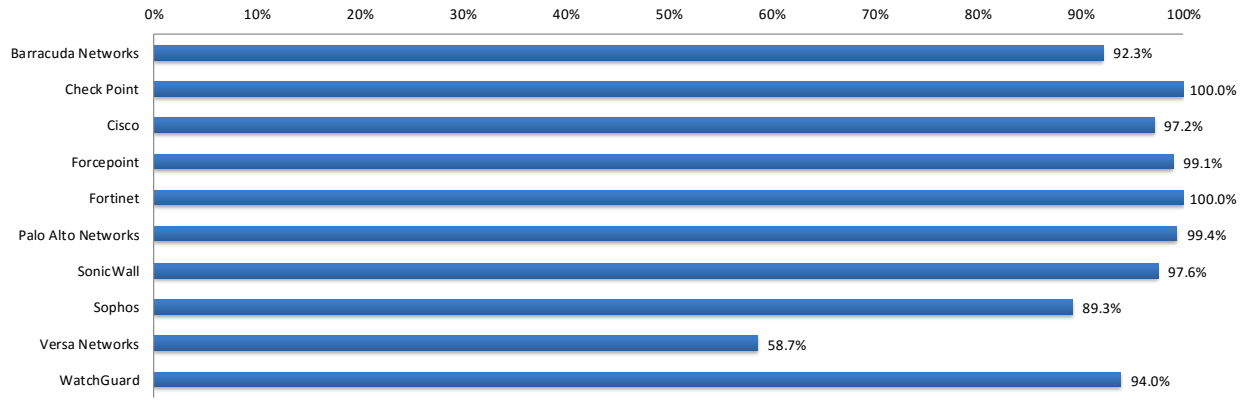

Figure 4 –Live Exploits

NSS 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 1,900 exploits, this is the industry's most comprehensive test to date.

Exploit Block Rate by Year

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

Vendor	Barracuda Networks	Check Point	Cisco	Forcepoint	Fortinet	Palo Alto Networks	SonicWall	Sophos	Versa Networks	WatchGuard
<=2008	98.1%	100.0%	99.3%	100.0%	99.8%	100.0%	99.1%	97.4%	100.0%	99.7%
2009	97.3%	100.0%	98.9%	100.0%	100.0%	100.0%	98.9%	96.8%	100.0%	98.4%
2010	96.0%	100.0%	97.9%	100.0%	100.0%	100.0%	98.8%	93.3%	99.4%	99.4%
2011	96.6%	100.0%	99.2%	100.0%	100.0%	100.0%	100.0%	84.7%	100.0%	99.2%
2012	96.6%	100.0%	99.0%	100.0%	100.0%	100.0%	99.5%	92.6%	100.0%	100.0%
2013	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	98.7%	100.0%	100.0%
2014	100.0%	100.0%	97.8%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
2015	96.8%	100.0%	86.3%	100.0%	100.0%	100.0%	98.9%	95.8%	97.9%	97.9%
2016	97.1%	100.0%	80.1%	100.0%	100.0%	100.0%	100.0%	99.6%	99.6%	98.9%
2017	93.3%	100.0%	86.7%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Resiliency	71.4%	75.8%	92.3%	96.7%	81.3%	67.0%	93.4%	65.9%	70.3%	69.2%
Total	96.2%	98.9%	95.3%	99.9%	99.1%	98.6%	99.1%	94.6%	98.5%	98.0%

Figure 5 – Exploit Block Rate by Year – Recommended Policies

Coverage by Attack Vector

Exploits can be initiated either locally by the target (desktop client) or remotely by the attacker against a server. 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 particulary 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, Firefox, QuickTime, and Microsoft Office applications.

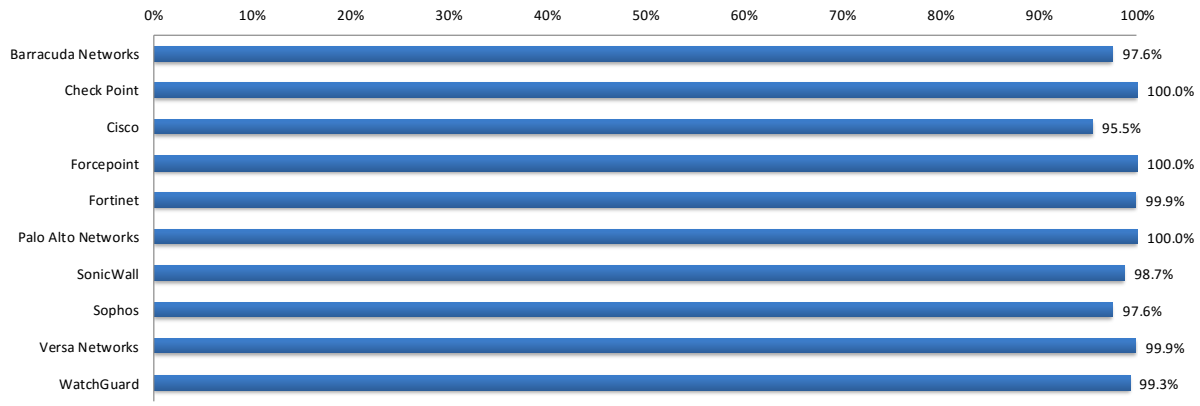

Figure 6 – Attacker-Initiated Exploit Block Rate (Server Side)

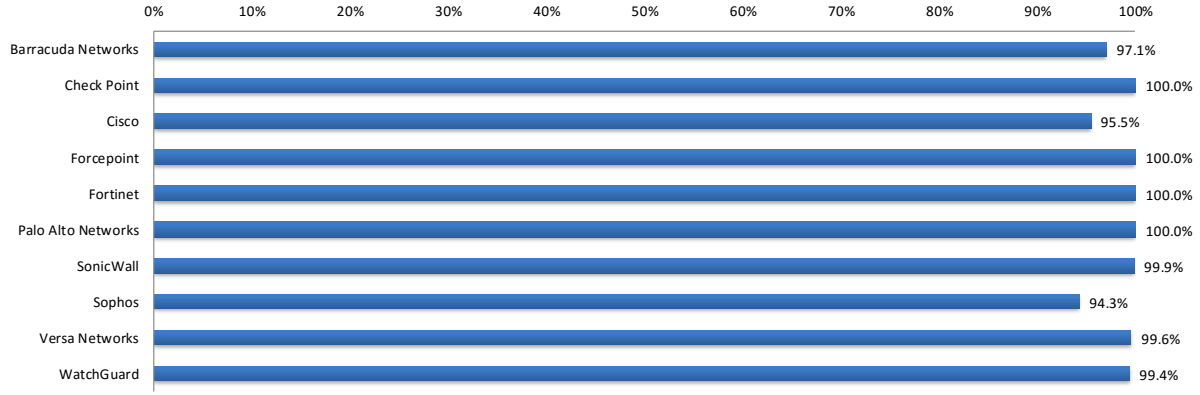

Figure 7 – Target-Initiated Exploit Block Rate (Client Side)

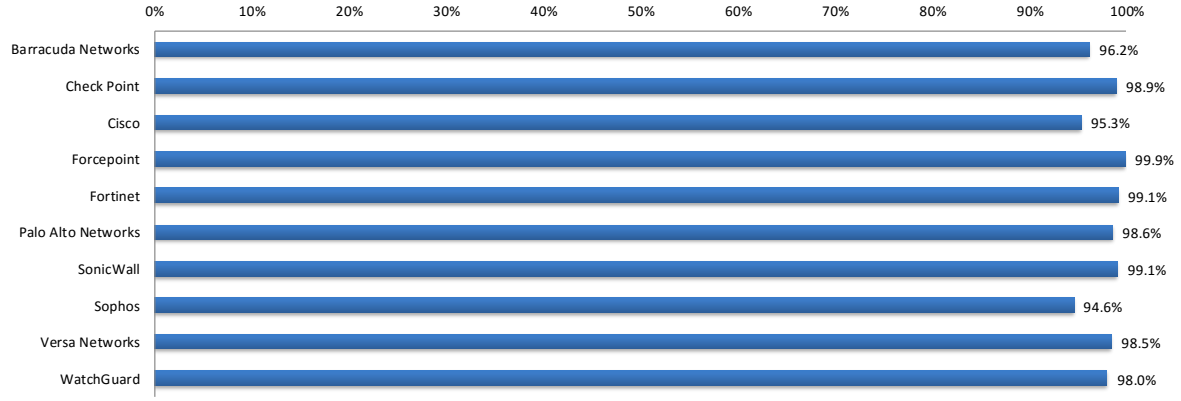

Figure 8 – Overall Exploit Block Rate

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.

Given the rapid evolution of criminal activity targeting desktop client applications, enterprises will need to dedicate more resources to client-side protection in 2018.

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.

Evasions

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.

TCP Split Handshake attacks can deceive the IPS engine into believing that the traffic flow is reversed and the IPS does not need to scan the content, which exposes the NGFW to previously known attacks.

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 will introduce various, previously unseen variations of exploits to exploit the vulnerability and measure the device's effectiveness against them. A resilient device will be able to detect and prevent against different variations of the exploit. A product's effectiveness is significantly handicapped if it fails to detect exploits that employ obfuscation or evasion techniques, and the NSS product guidance is adjusted to reflect this.

As with exploits, evasions can be employed specifically to obfuscate attacks that are initiated either locally by the target (client-side), or remotely by the attacker against a server (server-side). Some evasions are equally effective when used with both server-side *and* client-side attacks. See the *Coverage by Attack Vector* section of this report for more detail.

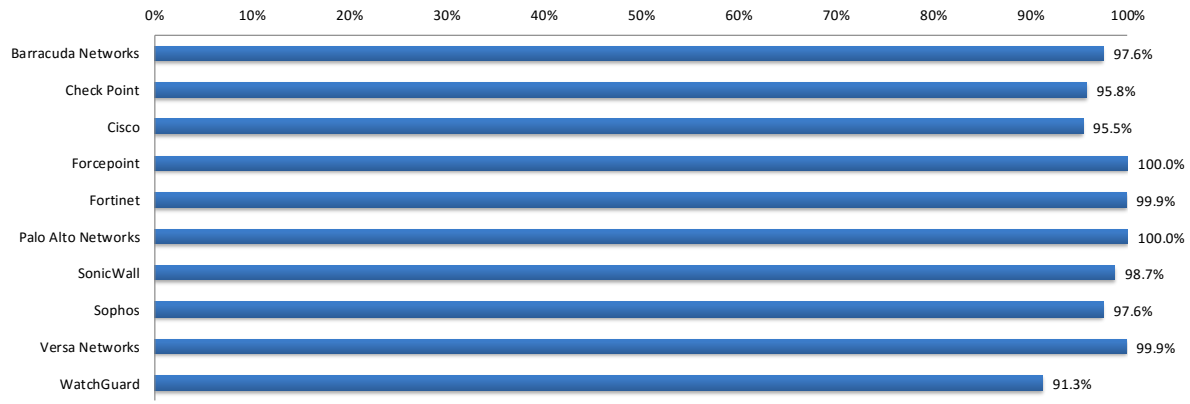

Figure 9 – Attacker-Initiated Exploits and Evasions (Server Side)

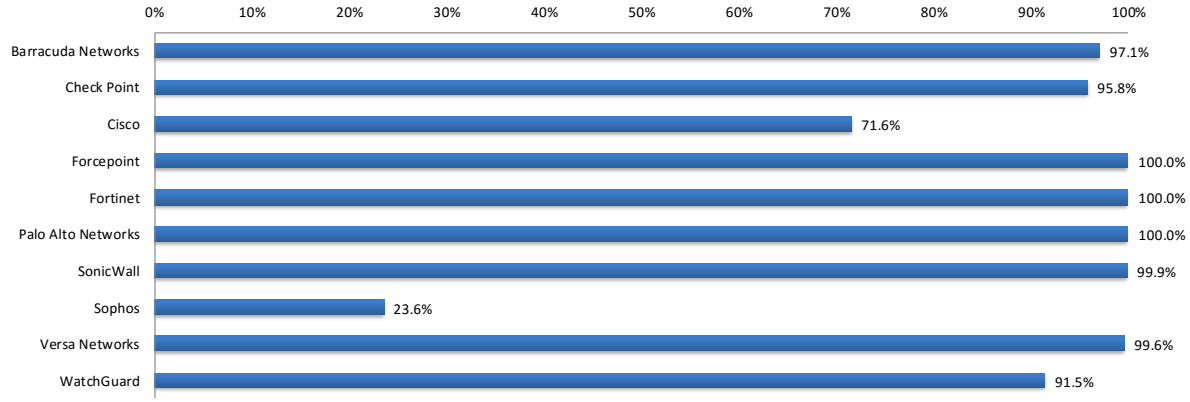

Figure 10 – Target-Initiated Exploits and Evasions (Client Side)

Figure 11 depicts how products fared against combinations of attacker-initiated exploits and evasions.

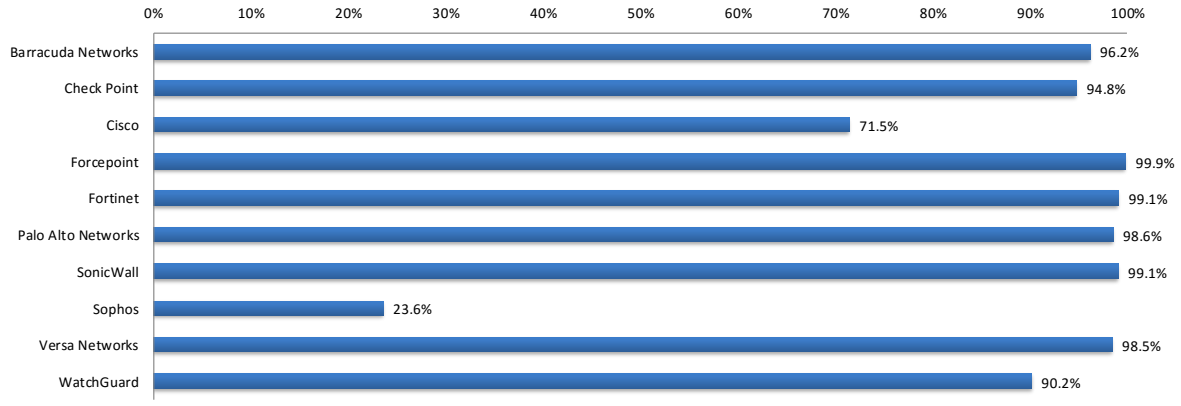

Figure 11 – Exploits and Evasions (Combined)

Figure 12 provides evasion resistance results for each the tested products. For additional details on which evasions were missed, see the individual Test Reports.

Vendor	Barracuda Networks	Check Point	Cisco	Forcepoint	Fortinet	Palo Alto Networks	SonicWall	Sophos	Versa Networks	WatchGuard
IP Packet Fragmentation/TCP Segmentation	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	FAIL
RPC Fragmentation	PASS	FAIL	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
URL Obfuscation	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
FTP/Telnet Evasion	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
HTTP Evasions	PASS	PASS	FAIL	PASS	PASS	PASS	PASS	PASS	PASS	PASS
HTML Evasions	PASS	PASS	PASS	PASS	PASS	PASS	PASS	FAIL	PASS	PASS
TCP Split Handshake	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Resiliency	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Attacks on nonstandard ports	FAIL	PASS	FAIL	PASS	PASS	FAIL	PASS	FAIL	PASS	FAIL

Figure 12 – Evasion Resistance

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.

Vendor	Barracuda Networks	Check Point	Cisco	Forcepoint	Fortinet	Palo Alto Networks	SonicWall	Sophos	Versa Networks	WatchGuard
Blocking under Extended Attack	PASS	FAIL	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Passing Legitimate Traffic under Extended Attack	PASS	FAIL	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Attack Detection/ Blocking – Normal Load	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
State Preservation – Normal Load	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Pass Legitimate Traffic – Normal Load	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
State Preservation – Maximum Exceeded	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Drop Traffic – Maximum Exceeded	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Power Fail	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Backup/Restore	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Persistence of Data	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Stability	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS

Figure 13 – 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	95.4%	100%	100%	95.4%
Check Point	99.2%	96%	25%	25.0%
Cisco	95.7%	75%	100%	71.8%
Forcepoint	99.7%	100%	100%	99.7%
Fortinet	99.3%	100%	100%	99.3%
Palo Alto Networks	98.7%	100%	100%	98.7%
SonicWall	98.8%	100%	100%	98.8%
Sophos	93.5%	25%	100%	25.0%
Versa Networks	90.4%	100%	100%	90.4%
WatchGuard	97.2%	92%	100%	89.1%

Figure 14 – Security Effectiveness

Test Methodology

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

Contact Information

3711 South Mopac Expressway
Building 1, Suite 400
Austin, TX 78746
info@nsslabs.com
www.nsslabs.com