NEXT GENERATION INTRUSION PREVENTION SYSTEM COMPARATIVE REPORT

Security

OCTOBER 13, 2016

Authors – Thomas Skybakmoen, Chris Conrad, Tim Otto, Morgan Dhanraj

Tested Products

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

Cisco FirePOWER 8350 v6.0.1

Forcepoint Stonesoft Next Generation Firewall 3301 v6.0.2

Fortinet FortiGate 3000D v5.4.0

IBM Security Network Protection XGS 7100 v5.3.2.1

Intel Security McAfee Network Security Platform NS9100 v8.2.5.158

Palo Alto Networks PA-7050 v7.0.4

Trend Micro TippingPoint 7500NX v3.8.4.4525

Environment

Next Generation Intrusion Prevention System Test Methodology v.2.0

Overview

Implementation of a next-generation intrusion prevention system (NGIPS) product can be a complex process, with multiple factors affecting the overall security effectiveness of the system.

The following factors should be considered over the course of the useful life of the NGIPS:

- Deployment use cases:
  - Will the NGIPS be deployed to protect servers, 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 NGIPS products 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 system under test (SUT).

Product	Exploit Block Rate	Anti-Evasion Rating	Stability and Reliability	Security Effectiveness
Check Point 13800	99.9%	100%	100%	99.9%
Cisco FirePOWER 8350	98.7%	100%	100%	98.7%
Forcepoint Stonesoft 3301	99.6%	100%	100%	99.6%
Fortinet FortiGate 3000D	99.8%	100%	25%	24.9%
IBM XGS 7100	94.4%	100%	100%	94.4%
Intel Security McAfee NS9100	98.5%	100%	100%	98.5%
Palo Alto Networks PA-7050	99.3%	100%	100%	99.3%
Trend Micro TippingPoint 7500NX	99.5%	100%	100%	99.5%

Figure 2 – Security Effectiveness

NGIPS products are deployed at the perimeter and within corporate networks to protect employee desktops, laptops, and PCs. NSS research has determined that the majority of enterprises do not tune their NGIPS products, but rather rely on a vendor's default/recommended policies and settings. Since there are enterprises that do tune their devices, NSS has tested NGIPS products using both tuned and vendor-recommended settings.

NSS defines a Vendor-Recommended policy as an out-of-the-box, vendor-pre-defined policy that is available to all customers. NSS defines tuning as the act of changing the device setting from the default/recommended setting to

[1] Exploit Block Rate is defined as the number of exploits blocked under test.

a specific configuration based on the environment it is protecting. In both cases, the signatures/filters/rules that trigger false positives are turned off, since that is what would happen in an enterprise environment.

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 NSS' Cyber Advanced Warning System (CAWS). Figure 3 depicts how each vendor scored against CAWS and the *NSS Exploit Library.*

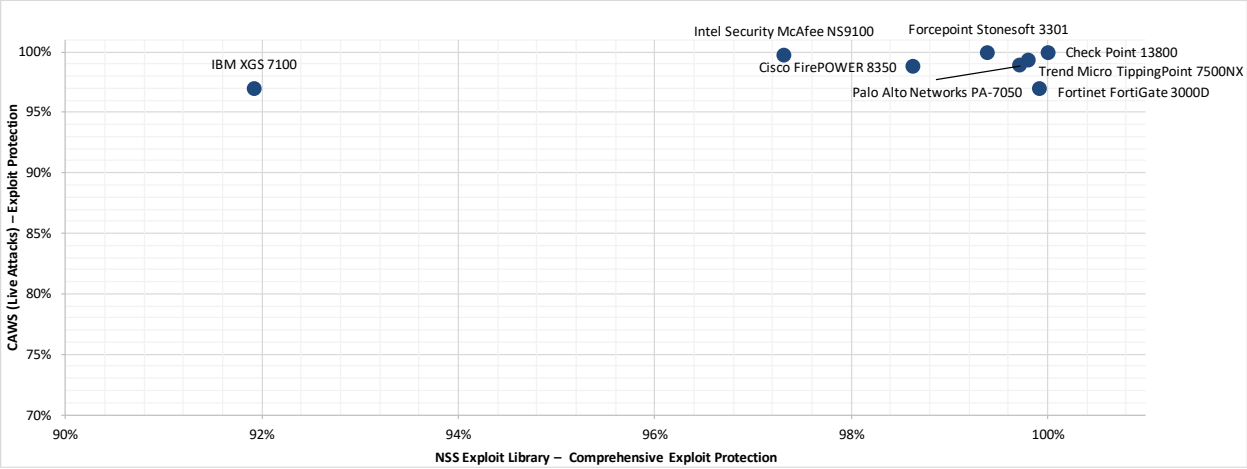

Figure 3 –CAWS (Live Attacks) and *NSS Exploit Library* Protection

Table of Contents

Table of Figures

Analysis

The threat landscape is evolving constantly; attackers are refining their strategies and increasing both the volume and intelligence of their attacks. Enterprises now must defend against targeted persistent attacks (TPA). In the past, servers were the main target. However, attacks against desktop client applications are now mainstream and present a clear danger to organizations.

CAWS (Live Exploits)

This test focuses on how effectively products are able to block attacks that are being 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. This means that there are three opportunities to break the chain of events leading to a successful compromise:

- URL access (reputation)
- Exploit
- Malware

Success or failure is based on whether or not the device blocks the attack. Attacks that are not successfully blocked are measured as a failure. For more information, see the Comparative Report on Security – CAWS (Live Exploits).

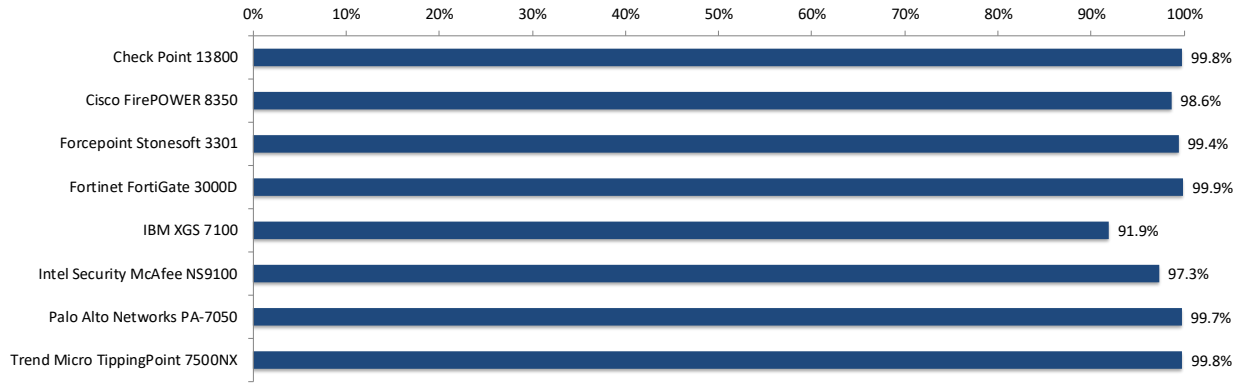

Figure 4 – CAWS (Live Exploits)

[2] See the NSS Cyber Advanced Warning System™ for more details.

NSS Exploit Library

NSS' security effectiveness testing leverages the deep expertise of our engineers, who utilize multiple commercial, open-source, and proprietary tools, including NSS' network live stack test environment[3] as appropriate. With 1986 exploits, this is the industry's most comprehensive test to date. Most notably, all of the exploits and payloads in this test have been validated such that:

- A reverse shell is returned
- A bind shell is opened on the target, allowing the attacker to execute arbitrary commands
- Arbitrary code is executed
- A malicious payload is installed
- A system is rendered unresponsive
- Etc.

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.

Where a product has performance limitations, vendors may retire older signatures in an attempt to alleviate those limitations; however, this may result in inconsistent coverage for older vulnerabilities and in varying levels of protection across products. Figure 5 and Figure 6 classify coverage by disclosure date, as tracked by CVE numbers. The heat maps in these figures are sorted by total protection, and the green sections of the heat maps indicate vendors with higher coverage for the given year (columns).

Product	<=2004	2005	2006	2007	2008	2009	2010
Check Point 13800	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	99.7%
Cisco FirePOWER 8350	92.9%	99.5%	99.5%	99.2%	98.7%	98.9%	97.9%
Forcepoint Stonesoft 3301	100.0%	99.5%	100.0%	100.0%	100.0%	100.0%	100.0%
Fortinet FortiGate 3000D	85.7%	100.0%	100.0%	100.0%	100.0%	100.0%	99.7%
IBM XGS 7100	92.9%	96.8%	96.3%	97.3%	96.8%	98.4%	96.6%
Intel Security McAfee NS9100	100.0%	98.9%	98.9%	99.6%	100.0%	100.0%	100.0%
Palo Alto Networks PA-7050	100.0%	97.9%	99.5%	100.0%	98.1%	97.3%	99.7%
Trend Micro TippingPoint 7500NX	100.0%	98.9%	98.4%	99.2%	99.7%	98.9%	99.1%

Figure 5 – Exploit Block Rate by Year – Recommended Policies (I)

[3] See the NSS Cyber Advanced Warning System™ for more details.

Product	2011	2012	2013	2014	2015	Total
Check Point 13800	100.0%	100.0%	100.0%	100.0%	100.0%	99.6%
Cisco FirePOWER 8350	98.3%	99.5%	100.0%	96.4%	96.8%	98.7%
Forcepoint Stonesoft 3301	100.0%	99.5%	100.0%	100.0%	100.0%	99.9%
Fortinet FortiGate 3000D	100.0%	100.0%	100.0%	100.0%	100.0%	99.8%
IBM XGS 7100	94.8%	97.5%	100.0%	95.2%	100.0%	97.0%
Intel Security McAfee NS9100	100.0%	100.0%	100.0%	100.0%	100.0%	99.7%
Palo Alto Networks PA-7050	98.3%	99.0%	100.0%	97.6%	100.0%	98.8%
Trend Micro TippingPoint 7500NX	100.0%	99.5%	100.0%	100.0%	100.0%	99.3%

Figure 6 – Exploit Block Rate by Year – Recommended Policies (II)

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 an unsuspecting user who visits an infected website. 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 NGIPS) industry has attempted to provide more complete client-side coverage. This is particularly important for NGIPS 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 as to when the target user or application will execute the threat. Target examples include Internet Explorer, Adobe Reader, Firefox, QuickTime, and Microsoft Office applications.

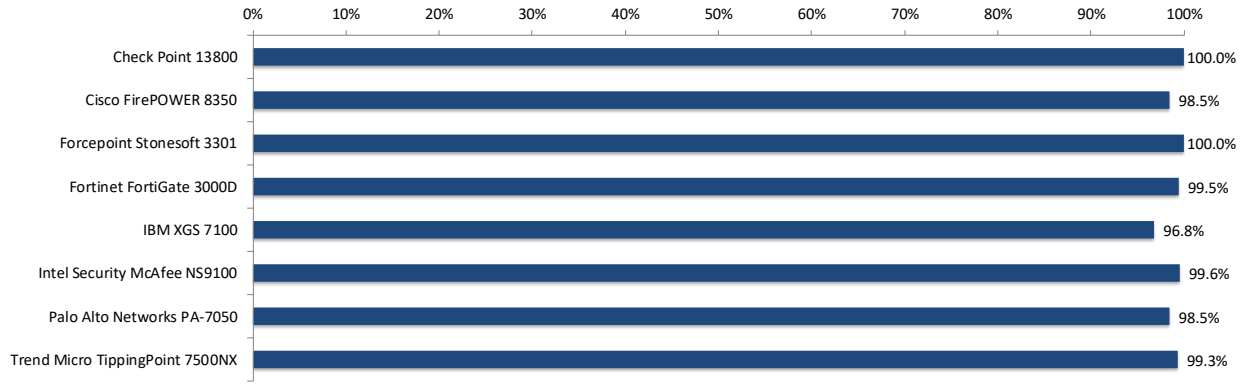

Figure 7 – Attacker-Initiated Exploit Block Rate

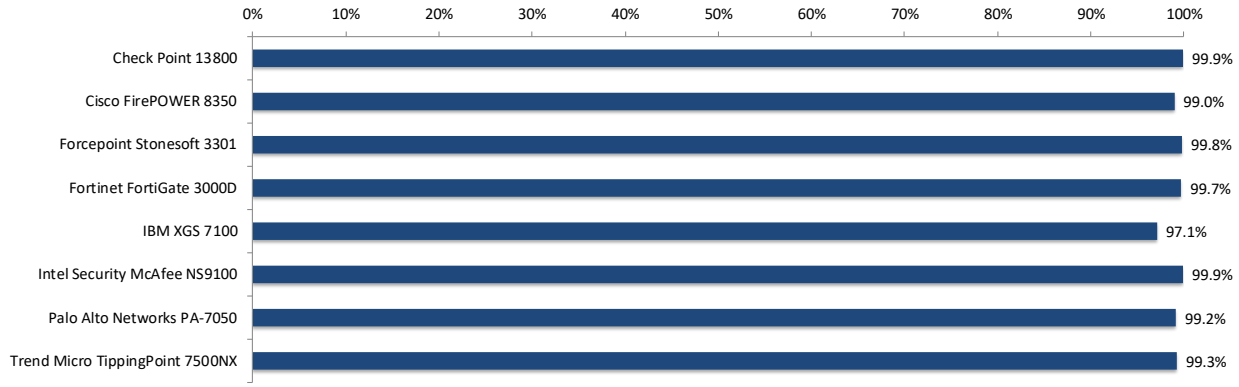

Figure 8 – Target-Initiated Exploit Block Rate

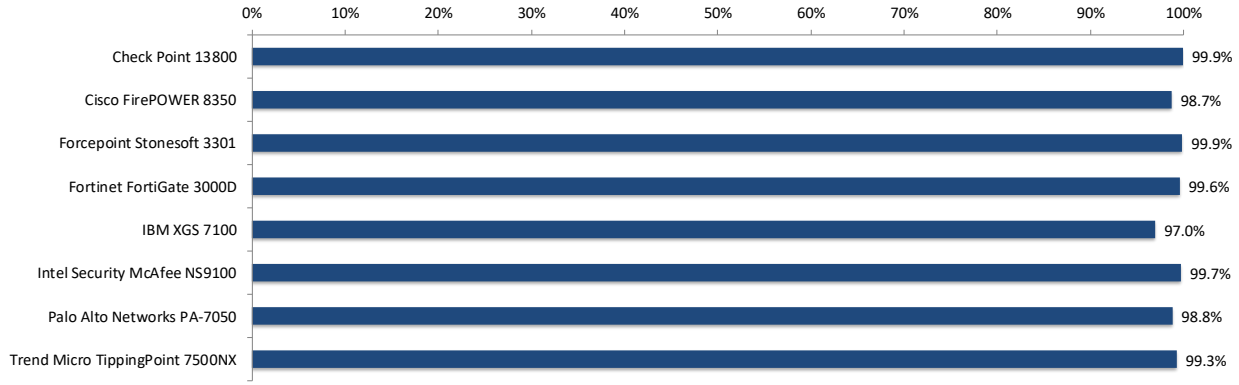

Figure 9 – Overall Exploit Block Rate

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.

Coverage by Target Vendor

Exploits within the *NSS Exploit Library* target a wide range of protocols and applications. Figure 10 depicts the coverage offered by each product for five of the top vendors targeted in this test. More than 50 vendors are represented in the test. Clients can contact NSS for more information.

Description	Adobe	Apple	IBM	Microsoft	Oracle
Check Point 13800	100.0%	100.0%	100.0%	99.9%	100.0%
Cisco FirePOWER 8350	98.2%	100.0%	100.0%	98.4%	100.0%
Forcepoint Stonesoft 3301	100.0%	100.0%	100.0%	99.9%	100.0%
Fortinet FortiGate 3000D	100.0%	100.0%	100.0%	99.9%	100.0%
IBM XGS 7100	96.5%	97.6%	98.6%	95.9%	99.1%
Intel Security McAfee NS9100	100.0%	100.0%	100.0%	99.6%	100.0%
Palo Alto Networks PA-7050	98.2%	100.0%	100.0%	99.1%	100.0%
Trend Micro TippingPoint 7500NX	100.0%	100.0%	100.0%	98.7%	100.0%

Figure 10 – Exploit Block Rate by Target Vendor

See the individual Test Reports for more information.

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 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 NGIPS product category.

Providing exploit protection results without fully factoring in evasion can be misleading. The more classes of evasion that are missed (such as IP packet fragmentation, stream segmentation, RPC fragmentation, URL obfuscation, HTML obfuscation, payload encoding, 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.

A product's effectiveness is significantly handicapped if it fails to detect exploits that employ obfuscation or evasion techniques.

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 section on Coverage by Attack Vector for more detail.

Figure 11 through Figure 13 depict attacker-initiated server-side exploits and evasions. Note that in this group test, none of the products missed any evasions.

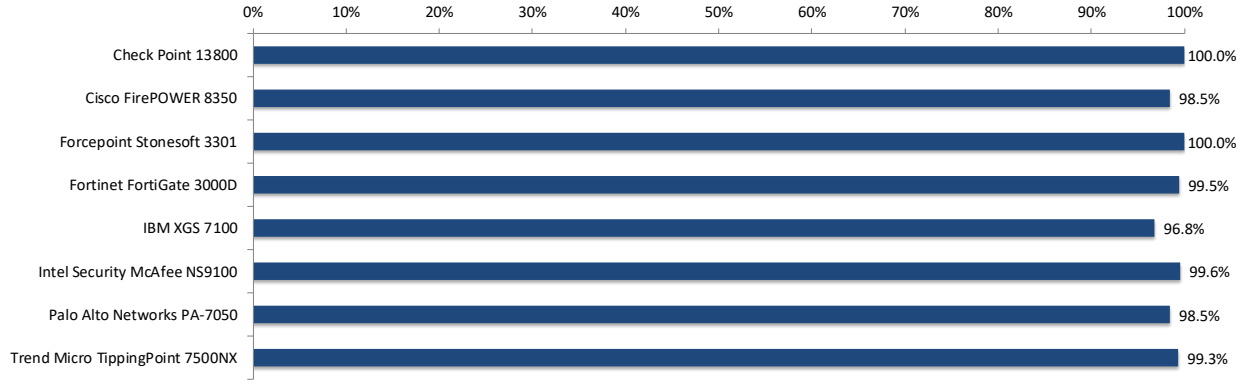

Figure 11 – Attacker-Initiated Exploits and Evasions (Server-side)

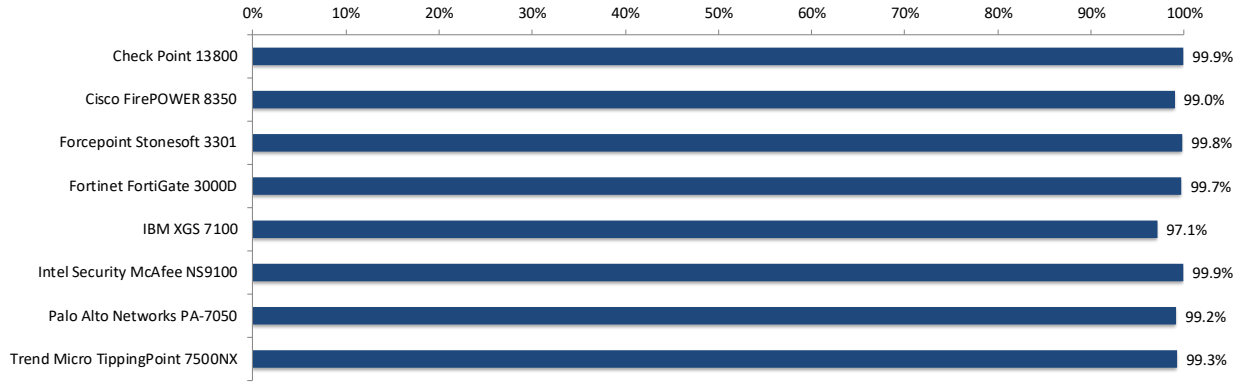

Figure 12 – Target-Initiated Exploits and Evasions

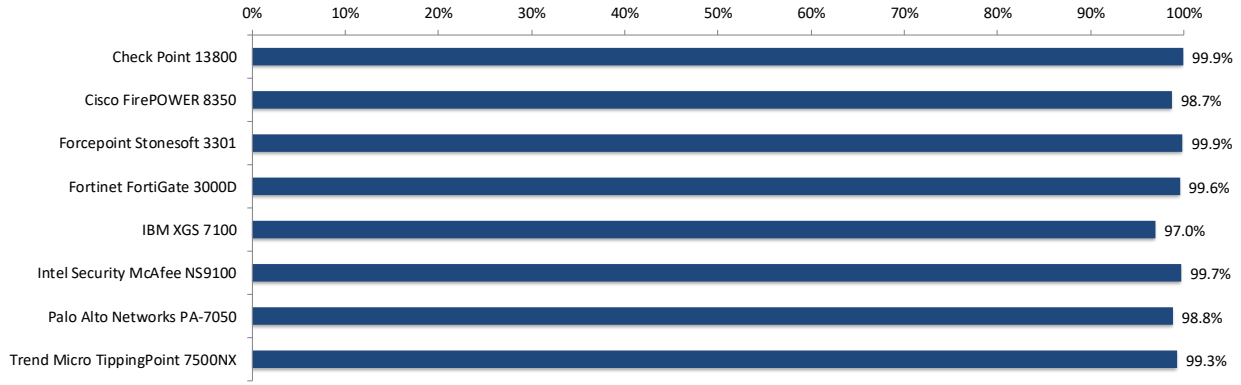

Figure 13 – Exploits and Evasions (Combined)

Figure 14 and Figure 15 provide details on evasion resistance for the tested products.

Product	IP Packet Fragmentation	Stream Segmentation	RPC Fragmentation	SMB & NetBIOS Evasions
Check Point 13800	PASS	PASS	PASS	PASS
Cisco FirePOWER 8350	PASS	PASS	PASS	PASS
Forcepoint Stonesoft 3301	PASS	PASS	PASS	PASS
Fortinet FortiGate 3000D	PASS	PASS	PASS	PASS
IBM XGS 7100	PASS	PASS	PASS	PASS
Intel Security McAfee NS9100	PASS	PASS	PASS	PASS
Palo Alto Networks PA-7050	PASS	PASS	PASS	PASS
Trend Micro TippingPoint 7500NX	PASS	PASS	PASS	PASS

Figure 14 – Evasion Resistance (I)

Product	URL Obfuscation	FTP Evasions	Payload Encoding	Layered Evasions
Check Point 13800	PASS	PASS	PASS	PASS
Cisco FirePOWER 8350	PASS	PASS	PASS	PASS
Forcepoint Stonesoft 3301	PASS	PASS	PASS	PASS
Fortinet FortiGate 3000D	PASS	PASS	PASS	PASS
IBM XGS 7100	PASS	PASS	PASS	PASS
Intel Security McAfee NS9100	PASS	PASS	PASS	PASS
Palo Alto Networks PA-7050	PASS	PASS	PASS	PASS
Trend Micro TippingPoint 7500NX	PASS	PASS	PASS	PASS

Figure 15 – Evasion Resistance (II)

Stability and Reliability

Long-term stability is particularly important for an inline device, where failure can produce network outages. These tests verify the stability of the SUT along with its ability to maintain security effectiveness while under normal load and while passing malicious traffic. Products that cannot sustain legitimate traffic (or that crash) while under hostile attack will not pass.

The device is required to remain operational and stable throughout these tests, and to block 100% of previously blocked traffic, raising an alert for each. If any non-allowed traffic passes successfully, caused either by the volume of traffic or by the SUT failing open for any reason, the device will fail the test.

Product	Blocking under Extended Attack	Passing Legitimate Traffic under Extended Attack	State Preservation – Normal Load	State Preservation – Maximum Exceeded
Check Point 13800	PASS	PASS	PASS	PASS
Cisco FirePOWER 8350	PASS	PASS	PASS	PASS
Forcepoint Stonesoft 3301	PASS	PASS	PASS	PASS
Fortinet FortiGate 3000D	PASS	PASS	PASS	FAIL
IBM XGS 7100	PASS	PASS	PASS	PASS
Intel Security McAfee NS9100	PASS	PASS	PASS	PASS
Palo Alto Networks PA-7050	PASS	PASS	PASS	PASS
Trend Micro TippingPoint 7500NX	PASS	PASS	PASS	PASS

Figure 16 – Stability and Reliability (I)

Product	Protocol Fuzzing and Mutation	Power Fail	Persistence of Data	Overall Stability and Reliability Score
Check Point 13800	PASS	PASS	PASS	PASS
Cisco FirePOWER 8350	PASS	PASS	PASS	PASS
Forcepoint Stonesoft 3301	PASS	PASS	PASS	PASS
Fortinet FortiGate 3000D	PASS	PASS	PASS	FAIL
IBM XGS 7100	PASS	PASS	PASS	PASS
Intel Security McAfee NS9100	PASS	PASS	PASS	PASS
Palo Alto Networks PA-7050	PASS	PASS	PASS	PASS
Trend Micro TippingPoint 7500NX	PASS	PASS	PASS	PASS

Figure 17 – Stability and Reliability (II)

Security Effectiveness

The *Security Effectiveness* of a device is determined by factoring the results of evasions testing and stability and reliability testing into the exploit block rate.

Product	Exploit Block Rate	Anti-Evasion Rating	Stability and Reliability	Security Effectiveness
Check Point 13800	99.9%	100%	100%	99.9%
Cisco FirePOWER 8350	98.7%	100%	100%	98.7%
Forcepoint Stonesoft 3301	99.6%	100%	100%	99.6%
Fortinet FortiGate 3000D	99.8%	100%	25%	24.9%
IBM XGS 7100	94.4%	100%	100%	94.4%
Intel Security McAfee NS9100	98.5%	100%	100%	98.5%
Palo Alto Networks PA-7050	99.3%	100%	100%	99.3%
Trend Micro TippingPoint 7500NX	99.5%	100%	100%	99.5%

Figure 18 – Security Effectiveness

Test Methodology

Next Generation Intrusion Prevention System Test Methodology v.2.0

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