DATA CENTER INTRUSION PREVENTION SYSTEM COMPARATIVE REPORT

Security

Authors – Thomas Skybakmoen, Keith Bormann, Morgan Dhanraj

Tested Products

Fortinet FortiGate 3000D v5.4.0, build 7184

HPE TippingPoint S7500NX v3.7.2.4252

IBM Security Network Protection XGS 7100 v5.3.2.1

Intel Security McAfee Network Security Platform NS9100 v8.2.5.120

Juniper Networks SRX5400 v12.3X48-D18

Palo Alto Networks PA-7050 v7.0.4

Environment

Data Center Intrusion Prevention System: Test Methodology v.2.0

Overview

Implementation of a data center intrusion prevention system (DCIPS) 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 DCIPS:

- Deployment use cases: 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 DCIPS 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 device under test (DUT).

Product	Exploit Block Rate	Anti-Evasion Rating	Stability and Reliability	Security Effectiveness
Fortinet FortiGate 3000D	99.9%	100%	100%	99.9%
HPE TippingPoint S7500NX	97.9%	95%	25%	23.2%
IBM XGS 7100	99.6%	100%	100%	99.6%
Intel Security McAfee NS9100	99.4%	100%	100%	99.4%
Juniper Networks SRX5400	98.7%	100%	100%	98.7%
Palo Alto Networks PA-7050	94.2%	100%	100%	94.2%

Figure 2 – Security Effectiveness

NSS research indicates that the majority of enterprises tune their DCIPS products. Therefore, NSS tests DCIPS products that have been optimally tuned by the vendor. Every effort is made to deploy policies that ensure the optimal combination of security effectiveness and performance, as would be the aim of a typical customer deploying the device in a live network environment.

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

IPS devices deployed within a data center typically are subjected to significantly higher traffic levels than are IPS or next generation firewalls (NGFWs) deployed at the corporate network perimeter. Furthermore, data center traffic mixes are significantly different from network perimeter traffic mixes. Where perimeter devices are expected to protect a wide range of end user applications, a data center device may be deployed to protect a single type of server, supporting far fewer network protocols and applications. Latency is also a concern since applications will be adversely affected if the IPS introduces delays. 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 DCIPS product category.

Figure 3 depicts the relationship between protection and performance when tuned policies are used. Farther up indicates better security effectiveness, and farther to the right indicates higher throughput.

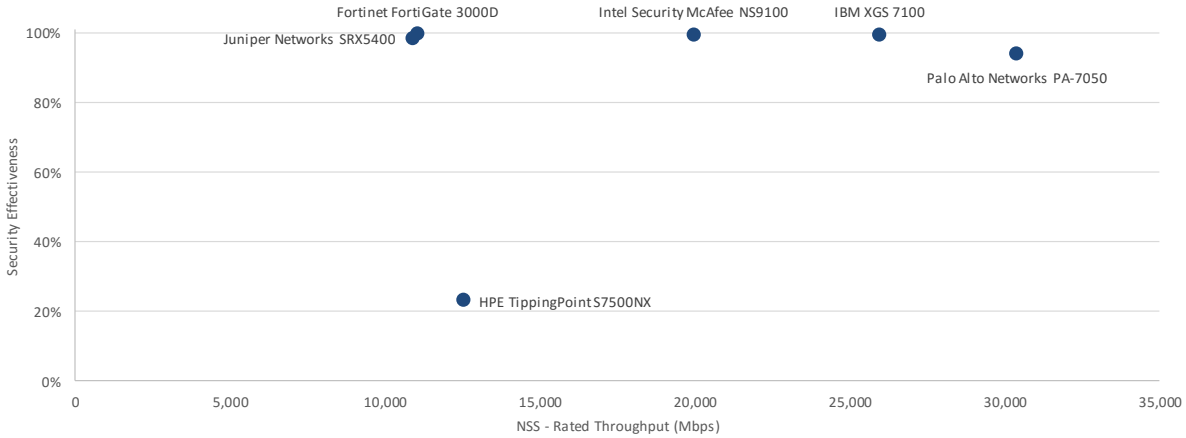

Figure 3 – Security Effectiveness and Performance

When selecting products, prioritize those that fall along the top line of the chart (closer to 100% security effectiveness). The throughput is a secondary consideration and will be dependent on enterprise-specific deployment requirements.

Table of Contents

Table of Figures

Analysis

The threat landscape is evolving constantly; attackers are refining their strategies and increasing both the volume and the intelligence of their attacks. Enterprises now must defend against targeted persistent attacks (TPAs). Although attacks against desktop client applications are mainstream in typical enterprise perimeter deployments, servers will always be the primary target in a data center deployment, and therefore tuning is critical.

Tuning

NSS research indicates that the majority of enterprises tune their DCIPS products. Therefore, NSS tests DCIPS products that have been optimally tuned by the vendor. Every effort is made to deploy policies that ensure the optimal combination of security effectiveness and performance, as would be the aim of a typical customer deploying the device in a live network environment.

IPS devices deployed within a data center typically are subjected to significantly higher traffic levels than are IPS or next generation firewalls (NGFWs) deployed at the corporate network perimeter. Furthermore, data center traffic mixes are significantly different from network perimeter traffic mixes. Where perimeter devices are expected to protect a wide range of end user applications, a data center device may be deployed to protect a single type of server, supporting far fewer network protocols and applications. Latency is also a concern since applications will be adversely affected if the IPS introduces delays. 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 DCIPS product category.

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[2] as appropriate. With 896 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.

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

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 4 and Figure 5 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
Fortinet FortiGate 3000D	100.0%	100.0%	100.0%	100.0%	99.3%	100.0%	100.0%
HPE TippingPoint S7500NX	100.0%	100.0%	97.4%	98.2%	97.0%	93.4%	99.2%
IBM XGS 7100	100.0%	99.0%	100.0%	100.0%	98.5%	100.0%	99.2%
Intel Security McAfee NS9100	100.0%	100.0%	98.7%	100.0%	100.0%	100.0%	100.0%
Juniper Networks SRX5400	100.0%	97.0%	100.0%	100.0%	97.8%	98.4%	100.0%
Palo Alto Networks PA-7050	100.0%	97.0%	94.9%	96.4%	95.5%	88.5%	97.5%

Figure 4 – Exploit Block Rate by Year – Recommended Policies (I)

Product	2011	2012	2013	2014	2015	Total
Fortinet FortiGate 3000D	100.0%	100.0%	100.0%	100.0%	100.0%	99.9%
HPE TippingPoint S7500NX	97.4%	97.5%	98.7%	100.0%	96.3%	97.9%
IBM XGS 7100	100.0%	100.0%	100.0%	100.0%	100.0%	99.6%
Intel Security McAfee NS9100	94.7%	97.5%	100.0%	100.0%	100.0%	99.4%
Juniper Networks SRX5400	97.4%	98.8%	98.7%	100.0%	96.3%	98.7%
Palo Alto Networks PA-7050	92.1%	90.1%	98.7%	92.3%	81.5%	94.2%

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

Coverage by Attack Vector

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). DCIPS security effectiveness tests focus on server-side attacks.
- Target-initated 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.

While client-side attacks are on the rise in the enterprise, the typical data center will only be vulnerable to server-side (attacker-initiated) attacks.

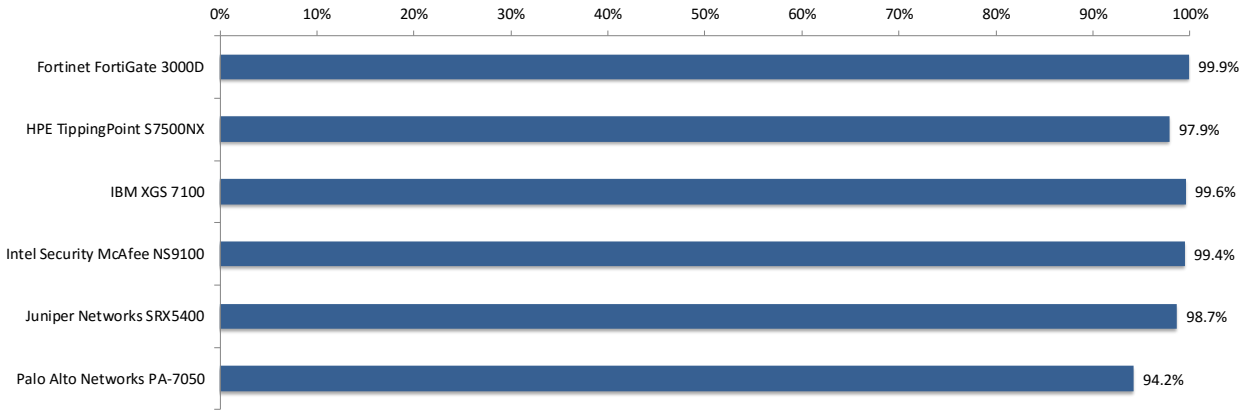

Figure 6 – Attacker-Initiated Exploit Block Rate

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 7 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	Apache	CA	EMC	HP	IBM
Fortinet FortiGate 3000D	100.0%	100.0%	100.0%	100.0%	100.0%
HPE TippingPoint S7500NX	96.7%	98.0%	94.1%	100.0%	100.0%
IBM XGS 7100	100.0%	100.0%	100.0%	100.0%	100.0%
Intel Security McAfee NS9100	93.3%	100.0%	94.1%	100.0%	100.0%
Juniper Networks SRX5400	100.0%	98.0%	100.0%	98.8%	98.0%
Palo Alto Networks PA-7050	96.7%	94.0%	58.8%	95.3%	96.0%

Figure 7 – 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 DCIPS 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 8 depicts attacker-initiated exploits and evasions combined.

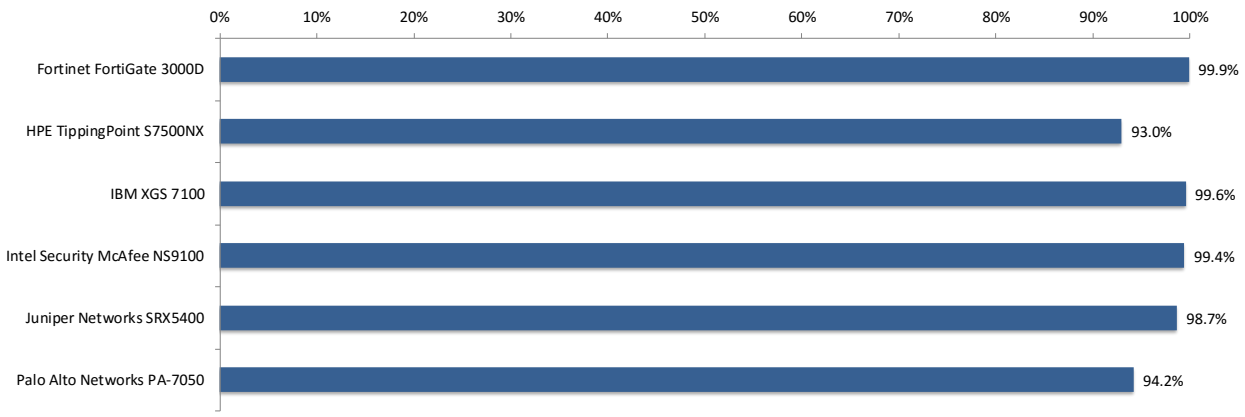

Figure 8 – Attacker-Initiated Exploits and Evasions

The following figures provide details on evasion resistance for the tested products. For additional details on which evasions were missed, see the corresponding Test Reports for each of the affected products.

Product	IP Packet Fragmentation	Stream Segmentation	RPC Fragmentation	URL Obfuscation	FTP Evasions	Layered Evasions
Fortinet FortiGate 3000D	PASS	PASS	PASS	PASS	PASS	PASS
HPE TippingPoint S7500NX	PASS	PASS	PASS	PASS	PASS	FAIL
IBM XGS 7100	PASS	PASS	PASS	PASS	PASS	PASS
Intel Security McAfee NS9100	PASS	PASS	PASS	PASS	PASS	PASS
Juniper Networks SRX5400	PASS	PASS	PASS	PASS	PASS	PASS
Palo Alto Networks PA-7050	PASS	PASS	PASS	PASS	PASS	PASS

Figure 9 – Evasion Resistance

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 DUT 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 DUT 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
Fortinet FortiGate 3000D	PASS	PASS	PASS	PASS
HPE TippingPoint S7500NX	PASS	PASS	FAIL	FAIL
IBM XGS 7100	PASS	PASS	PASS	PASS
Intel Security McAfee NS9100	PASS	PASS	PASS	PASS
Juniper Networks SRX5400	PASS	PASS	PASS	PASS
Palo Alto Networks PA-7050	PASS	PASS	PASS	PASS

Figure 10 – Stability and Reliability (I)

Product	Protocol Fuzzing and Mutation	Power Fail	Persistence of Data	Overall Stability and Reliability Score
Fortinet FortiGate 3000D	PASS	PASS	PASS	PASS
HPE TippingPoint S7500NX	PASS	PASS	PASS	FAIL
IBM XGS 7100	PASS	PASS	PASS	PASS
Intel Security McAfee NS9100	PASS	PASS	PASS	PASS
Juniper Networks SRX5400	PASS	PASS	PASS	PASS
Palo Alto Networks PA-7050	PASS	PASS	PASS	PASS

Figure 11 – 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
Fortinet FortiGate 3000D	99.9%	100%	100%	99.9%
HPE TippingPoint S7500NX	97.9%	95%	25%	23.2%
IBM XGS 7100	99.6%	100%	100%	99.6%
Intel Security McAfee NS9100	99.4%	100%	100%	99.4%
Juniper Networks SRX5400	98.7%	100%	100%	98.7%
Palo Alto Networks PA-7050	94.2%	100%	100%	94.2%

Figure 12 – Security Effectiveness

Test Methodology

Data Center Intrusion Prevention System v.2.0

A copy of the test methodology is available 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