NEXT GENERATION FIREWALL COMPARATIVE ANALYSIS

Security

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

Implementation of next generation firewall (NGFW) solutions can be a complex process with multiple factors affecting the overall *security effectiveness* of the solution. These should be considered over the course of the useful life of the solution, and include:

- Deployment use cases:
  - Will the NGFW be deployed to protect servers or desktop clients or both?
  - Age of 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 facilitate accurate product comparisons, NSS Labs has developed a unique metric:

Security Effectiveness = Firewall *(Firewall Policy Enforcement x Application Control x User/Group ID) x* ***IPS*** *(Exploit Block Rate*[1] ***x*** *Evasions)* ***x Stability and Reliability***

Figure 1 – Security Effectiveness Formula

By focusing on overall *security effectiveness* instead of the 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.

Product	Firewall	IPS	Stability and Reliability	Security Effectiveness
Barracuda F800b	100%	89.7%	100%	89.7%
Check Point 13500	100%	96.4%	100%	96.4%
Cisco ASA 5525-X	100%	99.2%	100%	99.2%
Cisco ASA 5585-X SSP60	100%	99.2%	100%	99.2%
Cisco FirePOWER 8350	100%	99.2%	100%	99.2%
Cyberoam CR2500iNG-XP	100%	88.2%	100%	88.2%
Dell SonicWALL SuperMassive E10800	100%	97.9%	100%	97.9%
Fortinet FortiGate-1500D	100%	94.1%	100%	94.1%
Fortinet FortiGate-3600C	100%	96.3%	100%	96.3%
McAfee NGF-1402	100%	95.5%	100%	95.5%
Palo Alto Networks PA-3020	100%	60.1%	100%	60.1%
WatchGuard XTM1525	100%	97.8%	100%	97.8%

Figure 2 – Security Effectiveness

NSS research indicates that the majority of enterprises will not tune the IPS portion of the NGFW. Therefore, in NSS' testing of NGFW products the devices are deployed using the default or recommended policy as provided by the vendor. Every effort is made to deploy policies that ensure the optimal combination of *security effectiveness*

[1] Exploit block rate is defined as the number of exploits blocked under test

and performance, as would be the aim of a typical customer deploying the device in a live network environment. This provides readers with the most useful information on key NGFW *security effectiveness* and performance capabilities based upon their expected usage.

Evasion techniques are a means of disguising and modifying attacks in order to avoid detection and blocking by security products. Resistance to evasion is a critical component in an NGFW. If a single evasion is missed, an attacker can utilize an entire class of exploits to circumvent the NGFW, rendering it 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, while others are more recent. This particular category of tests is critical in the final weighting with regard to product guidance. See Evasions chapter for more details.

Figure 3 depicts the relationship between protection and performance using default policies. Farther up indicates better *security effectiveness*, and farther to the right indicates higher throughput.

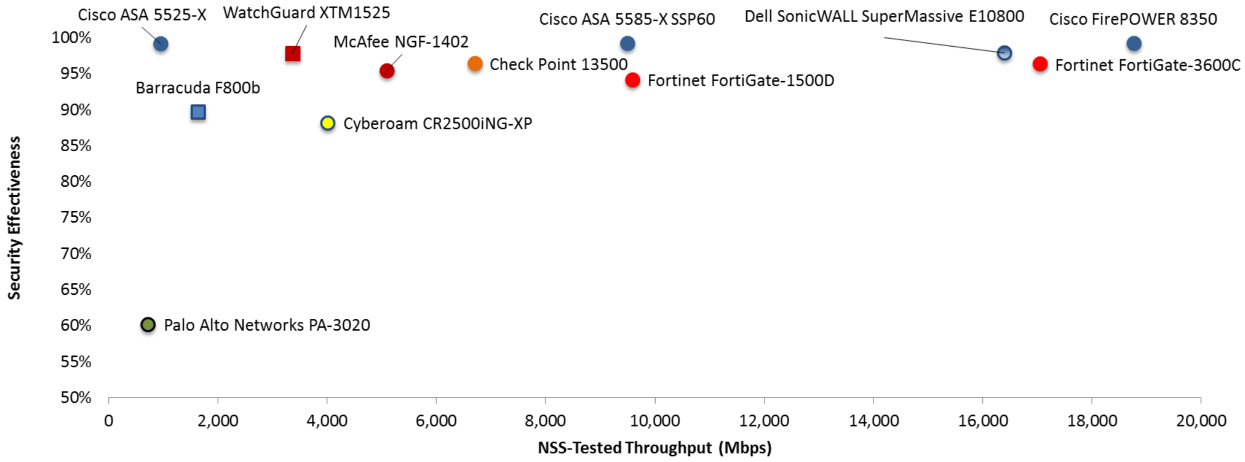


Figure 3 – Security Effectiveness and Performance

When selecting products, those along the top line of the chart (closer to 100% *security effectiveness*) should be prioritized. 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 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.

Tuning

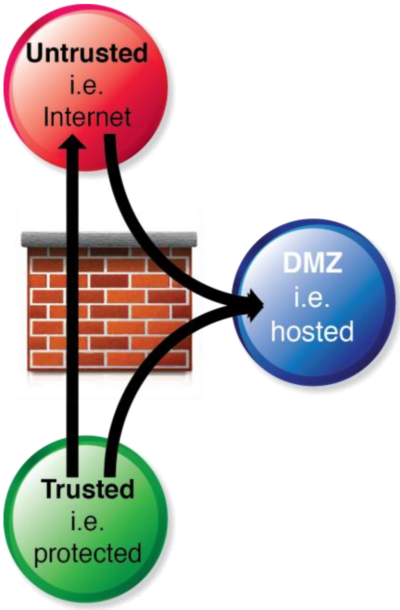
Security products are often complex, and vendors are responding by simplifying the user interface and security policy selection to meet the usability needs of a broadening user base. Whereas security engineers will typically tune an intrusion prevention system (IPS) to ensure its protection coverage matches the needs of the environment where it is being placed, NSS research shows that this is not the case with NGFW. In most cases, NGFW devices are deployed with the vendor-provided default or recommended policies in place. Enterprise users are expecting NGFW vendors in particular to provide maximum security for desktop client applications with these recommended policies.

For this reason, all testing was performed using the vendor-provided default or recommended policies. The only tuning permitted was to reconfigure any settings that resulted in false positive alerts that adversely affected the tests by blocking legitimate test traffic.

Firewall Policy Enforcement

Policies are rules that are configured on a firewall to permit or deny access from one network resource to another, based on identifying criteria such as source, destination, and service. A term typically used to define the demarcation point of a network where policy is applied is a *demilitarized zone* (DMZ). Policies are typically written to permit or deny network traffic from one or more of the following zones:

- **Untrusted –** This is typically an external network and is considered to be unknown and non-secure. An example of an untrusted network would be the Internet.
- **DMZ –** This is a network that is being *isolated* by the firewall restricting network traffic to and from hosts contained within the isolated network.
- **Trusted** – This is typically an internal network: a network that is considered secure and protected.



The NSS firewall tests verify performance and the ability to enforce policy between the following:

- Trusted to Untrusted
- Untrusted to DMZ
- Trusted to DMZ

Note: At a minimum, firewalls must provide one DMZ interface in order to provide a DMZ or “transition point” between untrusted and trusted networks.

Figure 4 and Figure 5 depicts the results from the firewall policy enforcement test.

Product	Baseline Policy	Simple Policy	Complex Policy	Static NAT	Dynamic / Hide NAT
Barracuda F800b	PASS	PASS	PASS	PASS	PASS
Check Point 13500	PASS	PASS	PASS	PASS	PASS
Cisco ASA 5525-X	PASS	PASS	PASS	PASS	PASS
Cisco ASA 5585-X SSP60	PASS	PASS	PASS	PASS	PASS
Cisco FirePOWER 8350	PASS	PASS	PASS	PASS	PASS
Cyberoam CR2500iNG-XP	PASS	PASS	PASS	PASS	PASS
Dell SonicWALL SuperMassive E10800	PASS	PASS	PASS	PASS	PASS
Fortinet FortiGate-1500D	PASS	PASS	PASS	PASS	PASS
Fortinet FortiGate-3600C	PASS	PASS	PASS	PASS	PASS
McAfee NGF-1402	PASS	PASS	PASS	PASS	PASS
Palo Alto Networks PA-3020	PASS	PASS	PASS	PASS	PASS
WatchGuard XTM1525	PASS	PASS	PASS	PASS	PASS

Figure 4 – Firewall Policy Enforcement (I)

Product	SYN Flood Protection	IP Address Spoofing Protection	TCP Split Handshake	Firewall Policy Protection
Barracuda F800b	PASS	PASS	PASS	PASS
Check Point 13500	PASS	PASS	PASS	PASS
Cisco ASA 5525-X	PASS	PASS	PASS	PASS
Cisco ASA 5585-X SSP60	PASS	PASS	PASS	PASS
Cisco FirePOWER 8350	PASS	PASS	PASS	PASS
Cyberoam CR2500iNG-XP	PASS	PASS	PASS	PASS
Dell SonicWALL SuperMassive E10800	PASS	PASS	PASS	PASS
Fortinet FortiGate-1500D	PASS	PASS	PASS	PASS
Fortinet FortiGate-3600C	PASS	PASS	PASS	PASS
McAfee NGF-1402	PASS	PASS	PASS	PASS
Palo Alto Networks PA-3020	PASS	PASS	PASS	PASS
WatchGuard XTM1525	PASS	PASS	PASS	PASS

Figure 5 — Firewall Policy Enforcement (II)

Application Control

An NGFW must provide granular control based upon applications, not just ports. This capability is needed to re-establish a secure perimeter where unwanted applications are unable to tunnel over HTTP/S. As such, granular application control is a requirement of an NGFW, since it enables the administrator to define security policies based upon applications rather than ports alone.

Product	Block Unwanted Applications	Block Specific Action	Application Control
Barracuda F800b	PASS	PASS	PASS
Check Point 13500	PASS	PASS	PASS
Cisco ASA 5525-X	PASS	PASS	PASS
Cisco ASA 5585-X SSP60	PASS	PASS	PASS
Cisco FirePOWER 8350	PASS	PASS	PASS
Cyberoam CR2500iNG-XP	PASS	PASS	PASS
Dell SonicWALL SuperMassive E10800	PASS	PASS	PASS
Fortinet FortiGate-1500D	PASS	PASS	PASS
Fortinet FortiGate-3600C	PASS	PASS	PASS
McAfee NGF-1402	PASS	PASS	PASS
Palo Alto Networks PA-3020	PASS	PASS	PASS
WatchGuard XTM1525	PASS	PASS	PASS

Figure 6 – Application Control

User/Group ID-Aware Policies

An NGFW should be able to identify users and groups and apply security policy based on identity. Where possible, this should be achieved via direct integration with existing enterprise authentication systems (such as Active Directory) without the need for custom server-side software. This allows the administrator to create even more granular policies.

Product	NGFW Integration with Active Directory	Users Defined in NGFW DB	User/Group ID Aware Policies
Barracuda F800b	PASS	N/A	PASS
Check Point 13500	PASS	N/A	PASS
Cisco ASA 5525-X	PASS	N/A	PASS
Cisco ASA 5585-X SSP60	PASS	N/A	PASS
Cisco FirePOWER 8350	PASS	N/A	PASS
Cyberoam CR2500iNG-XP	N/A	PASS	PASS
Dell SonicWALL SuperMassive E10800	N/A	PASS	PASS
Fortinet FortiGate-1500D	PASS	N/A	PASS
Fortinet FortiGate-3600C	PASS	N/A	PASS
McAfee NGF-1402	PASS	N/A	PASS
Palo Alto Networks PA-3020	PASS	N/A	PASS
WatchGuard XTM1525	N/A	PASS	PASS

Figure 7 – User Group ID-Aware Policies

Intrusion Prevention (IPS)

Exploit Block Rate

In order to represent accurately the protection that is likely to be achieved by a typical enterprise, NSS evaluates the DUT using the pre-defined default or recommended configuration that ships with the product “out-of-the-box.”

NSS’ *security effectiveness* testing leverages the deep expertise of NSS engineers to generate the same types of attacks used by modern cybercriminals, utilizing multiple commercial, open-source, and proprietary tools as appropriate. With over 1800 live exploits, this is the industry’s most comprehensive test to date. Most notable, all of the live exploits and payloads in these tests 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
- a malicious payload is installed
- the system is rendered unresponsive

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. An attempt 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 available to fully research a vulnerability will hopefully 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, resulting in inconsistent coverage for older vulnerabilities. This results in varying levels of protection across products. The following table classifies coverage by disclosure date, as tracked by CVE numbers. The table is sorted by total protection, and the green sections of the heat map indicate vendors with higher coverage for the given year (columns).

Product	<=2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	Total
Barracuda F800b	93.3%	88.5%	90.0%	91.6%	94.1%	93.0%	89.7%	72.6%	89.8%	72.0%	89.7%
Check Point 13500	100%	98.4%	100%	99.6%	99.4%	96.8%	94.6%	85.5%	94.1%	72.0%	96.4%
Cisco ASA 5525-X	100%	99.5%	100%	98.9%	99.7%	99.5%	99.7%	99.1%	97.6%	96.0%	99.2%
Cisco ASA 5585-X SSP60	100%	99.5%	100%	98.9%	99.7%	99.5%	99.7%	99.1%	97.6%	96.0%	99.2%
Cisco FirePOWER 8350	100%	99.5%	100%	98.9%	99.7%	99.5%	99.7%	99.1%	97.6%	96.0%	99.2%
Cyberoam CR2500iNG-XP	100%	99.0%	96.3%	97.3%	92.8%	94.6%	92.1%	77.8%	89.3%	64.0%	92.8%
Dell SonicWALL SuperMassive E10800	100%	97.9%	98.4%	98.9%	96.6%	97.3%	98.8%	96.6%	97.6%	100.0%	97.9%
Fortinet FortiGate-1500D	100%	98.4%	99.5%	97.7%	97.8%	97.3%	93.4%	72.6%	88.3%	68.0%	94.1%
Fortinet FortiGate-3600C	100%	98.4%	99.5%	97.7%	97.8%	97.3%	97.3%	85.5%	90.7%	96.0%	96.3%
McAfee NGF-1402	100%	97.9%	98.9%	98.1%	96.3%	98.9%	95.2%	83.8%	91.7%	76.0%	95.5%
Palo Alto Networks PA-3020	93.3%	96.9%	98.4%	98.9%	96.3%	95.1%	92.4%	75.2%	80.0%	64.0%	92.5%
WatchGuard XTM1525	100%	97.9%	94.2%	98.9%	100.0%	96.2%	97.3%	97.4%	98.5%	100%	97.8%

Figure 8 – Exploit Block Rate by Year – Recommended Policies

Exploit Block Rate 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, which were deemed to be 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 client-side coverage. 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.

NSS utilizes the following definitions:

Attacker-Initiated: The threat/exploit is executed by the attacker remotely 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: The threat/exploit is initiated by the vulnerable target (which is why these 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. These attacks traditionally target desktop client applications. Target examples include Internet Explorer, Adobe, Firefox, QuickTime, and Office applications.

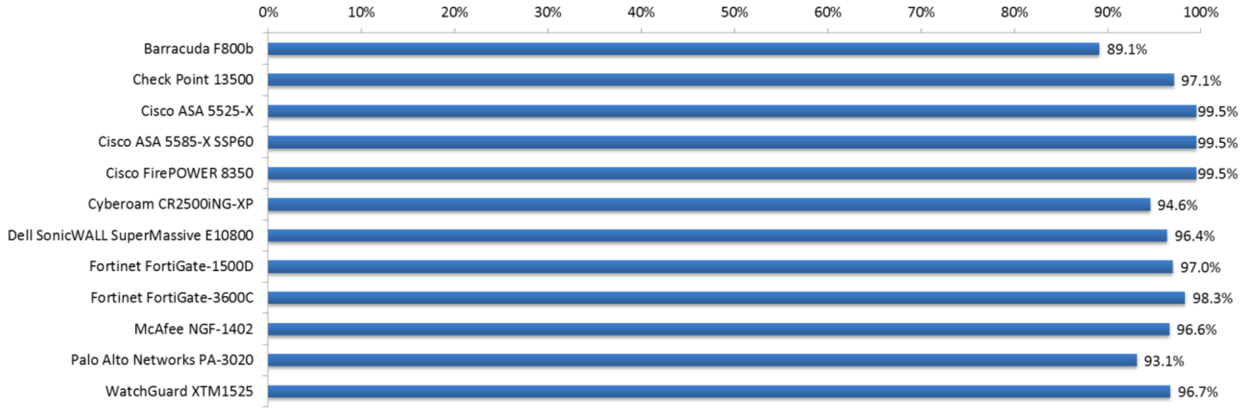


Figure 9 – Attacker-Initiated Exploit Block Rate (Server-Side)

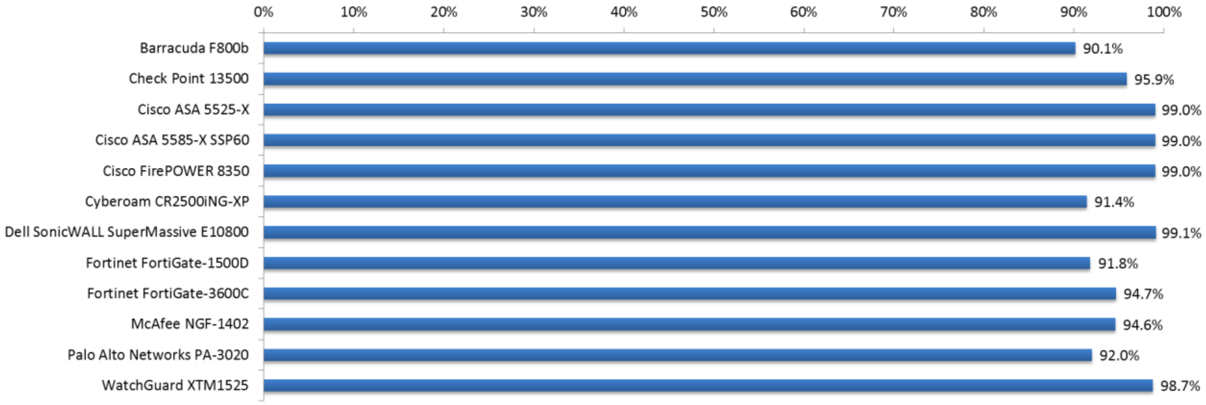


Figure 10 – Target-Initiated Exploit Block Rate (Client-Side)

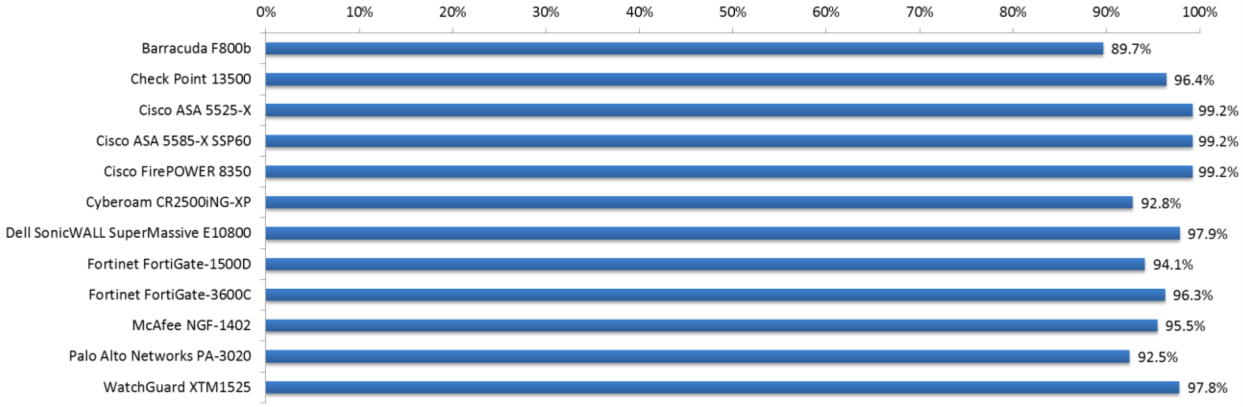


Figure 11 – Overall Exploit Block Rate

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 protecting servers in a DMZ or data center. Research also indicates that when it comes to protecting desktop client applications with an NGFW, enterprises are discovering that it is often best to enable a (nearly) full complement of signatures, since it is not feasible to tune an NGFW based upon 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 2014 and 2015.

Exploit Block Rate 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. Typical attacks in this category include service-specific attacks, such as SQL injection, that enable an attacker to execute arbitrary SQL commands within the database service. These attacks are somewhat isolated to the service and do not immediately result in full system-level access to the operating system and all services. However, by using additional localized system attacks, it may be possible for the attacker to escalate from the service level to the system level.

Finally, there are the attacks (often target initiated) which 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. These attacks do not enable the attacker to execute arbitrary commands. Still, the resulting impact to the business could be severe, as the attacker could crash a protected system or service.

Product	System Exposure	Service Exposure	System or Service Fault
Barracuda F800b	90.1%	90.0%	84.8%
Check Point 13500	96.0%	99.2%	98.6%
Cisco ASA 5525-X	99.1%	100.0%	100.0%
Cisco ASA 5585-X SSP60	99.1%	100.0%	100.0%
Cisco FirePOWER 8350	99.1%	100.0%	100.0%
Cyberoam CR2500iNG-XP	92.1%	97.5%	97.2%
Dell SonicWALL SuperMassive E10800	98.5%	95.0%	93.1%
Fortinet FortiGate-1500D	93.5%	99.2%	97.2%
Fortinet FortiGate-3600C	95.9%	99.2%	97.9%
McAfee NGF-1402	95.4%	97.5%	95.2%
Palo Alto Networks PA-3020	92.2%	97.5%	91.7%
WatchGuard XTM1525	98.1%	98.3%	94.5%

Figure 12 – Exploit Block Rate by Impact Type

Exploit Block Rate by Target Vendor

The NSS exploit library covers a wide range of protocols and applications representing a wide range of software vendors. This chart shows coverage for 5 of the top vendor targets (out of more than 70), as determined by the number of vendor-specific data center exploits in the NSS exploit library for this round of testing.

Description	Adobe	Apple	IBM	Microsoft	Oracle
Barracuda F800b	77.9%	98.8%	75.4%	88.9%	100.0%
Check Point 13500	79.1%	100.0%	95.4%	96.4%	100.0%
Cisco ASA 5525-X	98.8%	95.1%	96.9%	99.4%	99.0%
Cisco ASA 5585-X SSP60	98.8%	95.1%	96.9%	99.4%	99.0%
Cisco FirePOWER 8350	98.8%	95.1%	96.9%	99.4%	99.0%
Cyberoam CR2500iNG-XP	80.2%	96.3%	87.7%	91.4%	96.9%
Dell SonicWALL SuperMassive E10800	96.5%	100.0%	96.9%	98.5%	93.9%
Fortinet FortiGate-1500D	75.6%	95.1%	89.2%	93.0%	99.0%
Fortinet FortiGate-3600C	87.2%	95.1%	90.8%	96.0%	99.0%
McAfee NGF-1402	93.0%	98.8%	87.7%	94.2%	100.0%
Palo Alto Networks PA-3020	83.7%	98.8%	84.6%	91.1%	100.0%
WatchGuard XTM1525	100.0%	100.0%	98.5%	96.9%	99.0%

Figure 13 – Exploit Block Rate by Target Vendor

Evasions

Evasion techniques are a means of disguising and modifying attacks at the point of delivery in order to avoid detection and blocking by security products. Failure of a security device to handle correctly a particular type of evasion potentially will allow 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 NGFW product category.

Providing exploit protection results without fully factoring in evasion can be misleading. The more classes of evasion that are missed—IP packet fragmentation, TCP stream segmentation, RPC fragmentation, SMB and NetBIOS evasions, 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 (say, 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 fragmentation or TCP segmentation) will have a greater impact on *security effectiveness* than those operating at the upper layers (HTTP obfuscation or FTP evasion.) This is because lower-level evasions will impact potentially a wider number of exploits; therefore, missing TCP segmentation is a much more serious issue than missing FTP evasions.

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 section on *Exploit Block rate by Attack Vector* for more detail.

Figure 16 depicts attacker-initiated exploits and evasions combined.

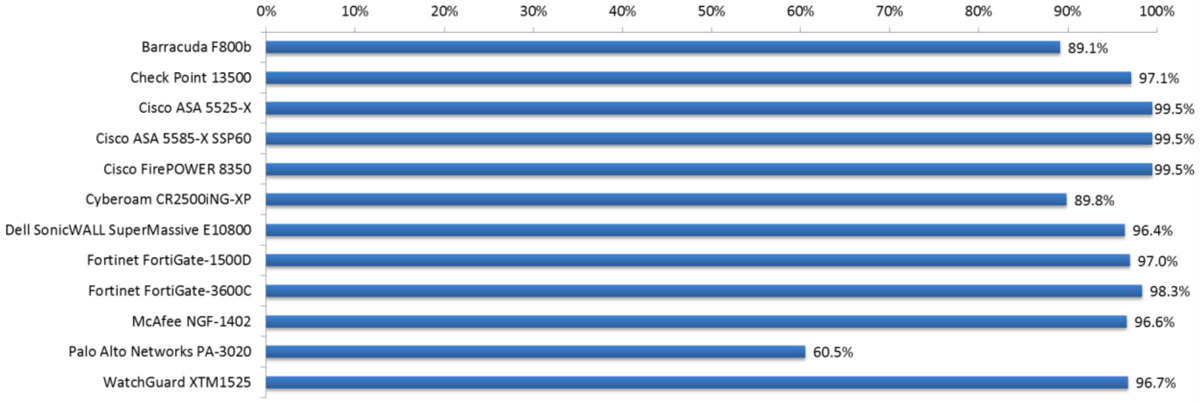


Figure 14 – Attacker-Initiated Exploits and Evasions (Server-Side)

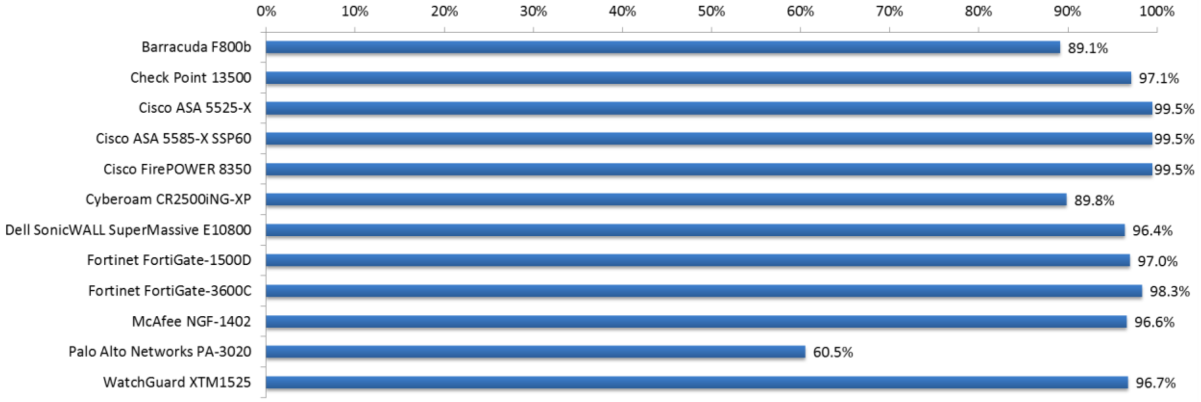


Figure 15 – Target-Initiated Exploits and Evasions (Client-Side)

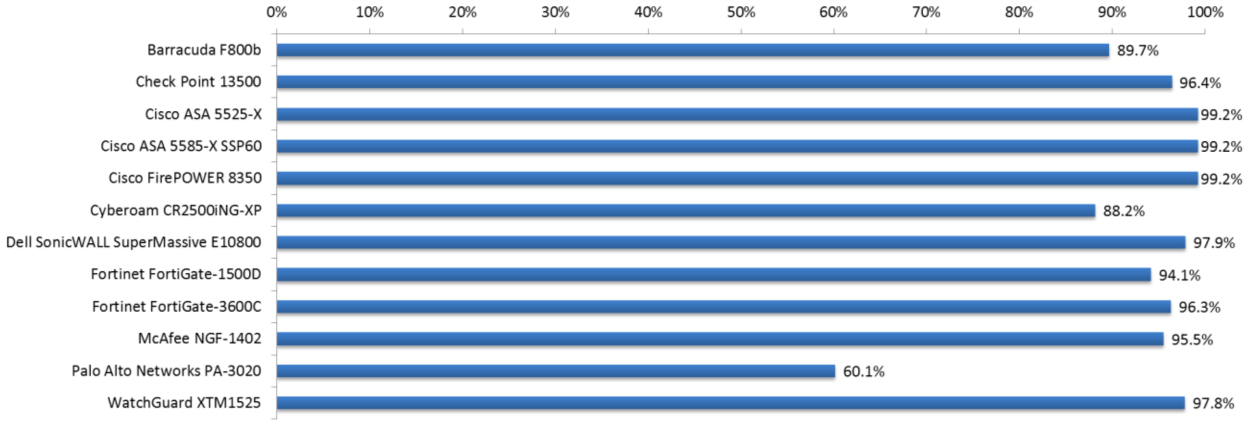


Figure 16 – Exploits and Evasions (Combined)

The following figures provide details on evasion resistance for the tested products.

Product	IP Packet Fragmentation	TCP Stream Segmentation	RPC Fragmentation	SMB & NetBIOS Evasions	URL Obfuscation
Barracuda F800b	PASS	PASS	PASS	PASS	PASS
Check Point 13500	PASS	PASS	PASS	PASS	PASS
Cisco ASA 5525-X	PASS	PASS	PASS	PASS	PASS
Cisco ASA 5585-X SSP60	PASS	PASS	PASS	PASS	PASS
Cisco FirePOWER 8350	PASS	PASS	PASS	PASS	PASS
Cyberoam CR2500iNG-XP	PASS	FAIL	PASS	PASS	PASS
Dell SonicWALL SuperMassive E10800	PASS	PASS	PASS	PASS	PASS
Fortinet FortiGate-1500D	PASS	PASS	PASS	PASS	PASS
Fortinet FortiGate-3600C	PASS	PASS	PASS	PASS	PASS
McAfee NGF-1402	PASS	PASS	PASS	PASS	PASS
Palo Alto Networks PA-3020	PASS	PASS	FAIL	PASS	PASS
WatchGuard XTM1525	PASS	PASS	PASS	PASS	PASS

Figure 17 – Evasion Resistance (I)

Product	HTML Obfuscation	Payload Encoding	FTP Evasion	IP Frag+ TCP Seg	IP Frag + MSRPC Frag
Barracuda F800b	PASS	PASS	PASS	PASS	PASS
Check Point 13500	PASS	PASS	PASS	PASS	PASS
Cisco ASA 5525-X	PASS	PASS	PASS	PASS	PASS
Cisco ASA 5585-X SSP60	PASS	PASS	PASS	PASS	PASS
Cisco FirePOWER 8350	PASS	PASS	PASS	PASS	PASS
Cyberoam CR2500iNG-XP	PASS	PASS	PASS	PASS	PASS
Dell SonicWALL SuperMassive E10800	PASS	PASS	PASS	PASS	PASS
Fortinet FortiGate-1500D	PASS	PASS	PASS	PASS	PASS
Fortinet FortiGate-3600C	PASS	PASS	PASS	PASS	PASS
McAfee NGF-1402	PASS	PASS	PASS	PASS	PASS
Palo Alto Networks PA-3020	PASS	PASS	PASS	FAIL	PASS
WatchGuard XTM1525	PASS	PASS	PASS	PASS	PASS

Figure 18 –Evasion Resistance (II)

Product	IP Fragmentation + SMB Evasions	TCP Segmentation + SMB / NETBIOS Evasions	Evasion Results
Barracuda F800b	PASS	PASS	100%
Check Point 13500	PASS	PASS	100%
Cisco ASA 5525-X	PASS	PASS	100%
Cisco ASA 5585-X SSP60	PASS	PASS	100%
Cisco FirePOWER 8350	PASS	PASS	100%
Cyberoam CR2500iNG-XP	PASS	PASS	95%
Dell SonicWALL SuperMassive E10800	PASS	PASS	100%
Fortinet FortiGate-1500D	PASS	PASS	100%
Fortinet FortiGate-3600C	PASS	PASS	100%
McAfee NGF-1402	PASS	PASS	100%
Palo Alto Networks PA-3020	PASS	PASS	65%
WatchGuard XTM1525	PASS	PASS	100%

Figure 19 –Evasion Results (Overall)

For additional details on which evasions were missed, see the corresponding PARs for each of the affected products.

Stability and Reliability

Long-term stability is particularly important for an in-line 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 are not able to sustain legitimate traffic (or that crash) while under hostile attack will not pass.

The DUT is required to remain operational and stable throughout these tests, and to block 100% of previously blocked traffic, raising an alert for each attack. If any prohibited traffic passes successfully, caused by either the volume of traffic or the device under test failing open for any reason, this will result in a FAIL.

Product	Blocking Under Extended Attack	Passing Legitimate Traffic Under Extended Attack	Attack Detection/Blocking Normal Load	State Preservation Normal Load	Pass Legitimate Traffic Normal Load
Barracuda F800b	PASS	PASS	PASS	PASS	PASS
Check Point 13500	PASS	PASS	PASS	PASS	PASS
Cisco ASA 5525-X	PASS	PASS	PASS	PASS	PASS
Cisco ASA 5585-X SSP60	PASS	PASS	PASS	PASS	PASS
Cisco FirePOWER 8350	PASS	PASS	PASS	PASS	PASS
Cyberoam CR2500iNG-XP	PASS	PASS	PASS	PASS	PASS
Dell SonicWALL SuperMassive E10800	PASS	PASS	PASS	PASS	PASS
Fortinet FortiGate-1500D	PASS	PASS	PASS	PASS	PASS
Fortinet FortiGate-3600C	PASS	PASS	PASS	PASS	PASS
McAfee NGF-1402	PASS	PASS	PASS	PASS	PASS
Palo Alto Networks PA-3020	PASS	PASS	PASS	PASS	PASS
WatchGuard XTM1525	PASS	PASS	PASS	PASS	PASS

Figure 20 – Stability and Reliability (I)

Product	State Preservation - Maximum Exceeded	Drop Traffic - Maximum Exceeded	Protocol Fuzzing & Mutation	Power Fail	Redundancy	Persistence of Data	Stability and Reliability
Barracuda F800b	PASS	PASS	PASS	PASS	YES	PASS	PASS
Check Point 13500	PASS	PASS	PASS	PASS	YES	PASS	PASS
Cisco ASA 5525-X	PASS	PASS	PASS	PASS	YES	PASS	PASS
Cisco ASA 5585-X SSP60	PASS	PASS	PASS	PASS	YES	PASS	PASS
Cisco FirePOWER 8350	PASS	PASS	PASS	PASS	YES	PASS	PASS
Cyberoam CR2500iNG-XP	PASS	PASS	PASS	PASS	YES	PASS	PASS
Dell SonicWALL SuperMassive E10800	PASS	PASS	PASS	PASS	YES	PASS	PASS
Fortinet FortiGate-1500D	PASS	PASS	PASS	PASS	YES	PASS	PASS
Fortinet FortiGate-3600C	PASS	PASS	PASS	PASS	YES	PASS	PASS
McAfee NGF-1402	PASS	PASS	PASS	PASS	YES	PASS	PASS
Palo Alto Networks PA-3020	PASS	PASS	PASS	PASS	NO	PASS	PASS
WatchGuard XTM1525	PASS	PASS	PASS	PASS	NO	PASS	PASS

Figure 21 – Stability and Reliability (II)

Redundancy is not factored into the final score. See methodology for more details.

Security Effectiveness

It is possible to rate the *security effectiveness* of the individual components of an NGFW. The *security effectiveness* of the firewall component of the NGFW can be seen in the following table as NSS factors in firewall policy enforcement to the application control and user/group ID capabilities.

Product	Firewall Policy Protection	Application Control	User/Group ID Aware Policies	Overall Firewall
Barracuda F800b	100%	100%	100%	100%
Check Point 13500	100%	100%	100%	100%
Cisco ASA 5525-X	100%	100%	100%	100%
Cisco ASA 5585-X SSP60	100%	100%	100%	100%
Cisco FirePOWER 8350	100%	100%	100%	100%
Cyberoam CR2500iNG-XP	100%	100%	100%	100%
Dell SonicWALL SuperMassive E10800	100%	100%	100%	100%
Fortinet FortiGate-1500D	100%	100%	100%	100%
Fortinet FortiGate-3600C	100%	100%	100%	100%
McAfee NGF-1402	100%	100%	100%	100%
Palo Alto Networks PA-3020	100%	100%	100%	100%
WatchGuard XTM1525	100%	100%	100%	100%

Figure 22 – Security Effectiveness (Firewall)

The *security effectiveness* of the IPS component of the NGFW can be seen in the following table as NSS factors in evasions to the exploit block rate.

Product	Exploit Block Rate	IPS Evasions	Overall IPS
Barracuda F800b	89.7%	100.0%	89.7%
Check Point 13500	96.4%	100.0%	96.4%
Cisco ASA 5525-X	99.2%	100.0%	99.2%
Cisco ASA 5585-X SSP60	99.2%	100.0%	99.2%
Cisco FirePOWER 8350	99.2%	100.0%	99.2%
Cyberoam CR2500iNG-XP	92.8%	95.0%	88.2%
Dell SonicWALL SuperMassive E10800	97.9%	100.0%	97.9%
Fortinet FortiGate-1500D	94.1%	100.0%	94.1%
Fortinet FortiGate-3600C	96.3%	100.0%	96.3%
McAfee NGF-1402	95.5%	100.0%	95.5%
Palo Alto Networks PA-3020	92.5%	65.0%	60.1%
WatchGuard XTM1525	97.8%	100.0%	97.8%

Figure 23 – Security Effectiveness (IPS)

Finally, the overall *security effectiveness* of the NGFW is determined using the formula in figure 1. Here, NSS combines scores relating to firewall *security effectiveness*, IPS *security effectiveness*, and stability and reliability in order to generate a combined *security effectiveness* score for the NGFW device.

Product	Firewall	IPS	Stability and Reliability	Security Effectiveness
Barracuda F800b	100%	90%	100%	89.7%
Check Point 13500	100%	96%	100%	96.4%
Cisco ASA 5525-X	100%	99%	100%	99.2%
Cisco ASA 5585-X SSP60	100%	99%	100%	99.2%
Cisco FirePOWER 8350	100%	99%	100%	99.2%
Cyberoam CR2500iNG-XP	100%	88%	100%	88.2%
Dell SonicWALL SuperMassive E10800	100%	98%	100%	97.9%
Fortinet FortiGate-1500D	100%	94%	100%	94.1%
Fortinet FortiGate-3600C	100%	96%	100%	96.3%
McAfee NGF-1402	100%	95%	100%	95.5%
Palo Alto Networks PA-3020	100%	60%	100%	60.1%
WatchGuard XTM1525	100%	98%	100%	97.8%

Figure 24 – Security Effectiveness (NGFW)

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
Building 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.

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.