WEB APPLICATION FIREWALL COMPARATIVE ANALYSIS

Security

Author – Thomas Skybakmoen

Tested Products

Barracuda Networks Web Application Firewall 960

Citrix NetScaler AppFirewall MPX 11520

Fortinet FortiWeb 1000D

F5 Big-IP ASM 10200

Imperva SecureSphere x6500

Sangfor M5900-F-I

Environment

Web Application Firewall: Test Methodology v6.2

Overview

Implementation of web application firewall (WAF) 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
  - What applications and web services will the WAF protect?
  - How old is the operating system?
  - How old are the applications?
- Defensive capabilities in the deployment use cases (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 *= Block Rate*[1] ***x*** *Anti-Evasion Rating* ***x*** *Stability and Reliability*

Figure 1 – Security Effectiveness Formula

By focusing on overall *security effectiveness* instead of the 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	Block Rate	Evasions	Stability and Reliability	Security Effectiveness
Barracuda Networks Web Application Firewall 960	99.97%	100%	100%	99.97%
Citrix NetScaler AppFirewall MPX 11520	99.77%	100%	100%	99.77%
Fortinet FortiWeb 1000D	99.85%	100%	100%	99.85%
F5 Big-IP ASM 10200	99.89%	100%	100%	99.89%
Imperva SecureSphere x6500	99.82%	100%	100%	99.82%
Sangfor M5900-F-I	96.11%	100%	100%	96.11%

Figure 2 – Security Effectiveness

NSS' research indicates that all enterprises tune their WAF devices. Therefore, for NSS' testing of WAF products, the devices are deployed using a tuned policy. 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. This provides readers with the most useful information on key WAF *security effectiveness* and performance capabilities, based on 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 a WAF. If a single evasion is missed, an attacker can utilize an entire class of attacks to circumvent the WAF, 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

[1] Block rate is defined as the number of attacks blocked under test

product category, while others are more recent. This particular category of tests is critical in the final weighting with regard to product guidance.

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 capacity (connections per second CPS)

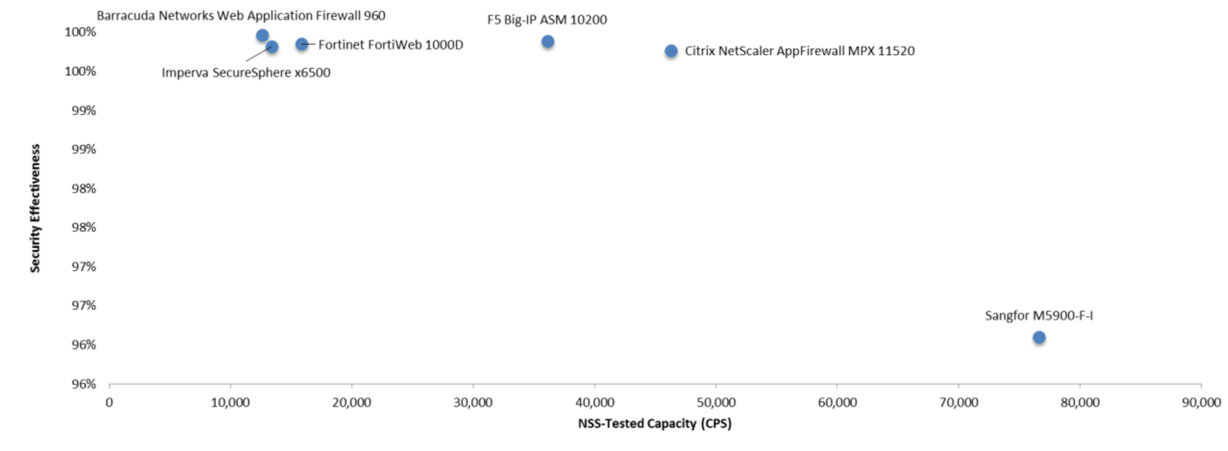

Figure 3 – Security Effectiveness and Performance

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

Table of Contents

Table of Figures

Analysis

Attackers have moved up the stack. They are no longer simply attacking the web server and its underlying operating systems, they are attacking the web applications running on the web server that are front-ending critical corporate data. Such applications are often incredibly complex and difficult to secure effectively, and simple coding errors can render them wide open to remote exploits.

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. Indeed, many organizations accept and deploy the default settings, understanding these to be the best recommendations from the vendor. In this, WAF is the exception to the rule. NSS' research indicated that most, if not all, enterprises tune their WAF. In general, accepting a vendor's defaults is likely to result in the omission of a significant number of deployment-specific signatures, which could leave an organization at risk. With the shortage of skilled and experienced practitioners, it is important to consider the time and resources required to properly install, maintain, and tune the solution. Failure to do so could result in products not achieving their full security potential. Therefore, all WAF products are tuned prior to testing to eliminate false positives and provide the most appropriate coverage for the systems to be protected.

NSS testing has found that the majority of web application firewalls (WAFs) operate in an adaptive learning mode ("learning mode"). In this mode, a WAF learns the behavior of applications and automatically generates policy recommendations. These recommendations require review and approval before the WAF device is deployed. Periodic manual tuning may also be required.

Typically, tuning is carried out by experienced system engineers from the vendor company, but where this is not possible, NSS engineers will perform the necessary tuning. NSS engineers may also amend the configuration of a device under test (DUT), where specific characteristics of the DUT or its configuration interfere with the normal operation of any of the tests, or where the results obtained from those tests would, in the opinion of those engineers, misrepresent the true capabilities of the DUT. Every effort is made to ensure the optimal combination of *security effectiveness* and performance, as would be the aim of a typical customer deploying the DUT in a live network environment.

Attack Types

The NSS threat and attack suite contains thousands of publically available exploits (including multiple variants of each exploit) and a number of complex web applications that have been constructed to include known vulnerabilities and coding errors. Groups of exploits are carefully selected from this library to test based on the intended attack type as listed below. Each exploit has been validated to impact the target vulnerable host(s) by compromising either the underlying OS, the web server, or the web application itself.

Attack types:

- **URL Parameter Manipulation –** altering URL data to gain potentially protected information or access protected areas of a website.
- **Form/Hidden Field Manipulation —** constructing POST requests to access protected information or protected areas of a website, or to manipulate "fixed" data directly (such as pricing information).
- **Cookie/Session Poisoning —** manipulation of cookie or session variables to access protected information or protected areas of a website.
- **Cross-Site Scripting (XSS) —** the process of manipulating user input in such a way that, when rendered in the context of a webpage, it will be interpreted by the browser as code.
- **Directory traversal —** altering the URL to access areas of the web server that should not otherwise be accessible.
- **SQL Injection —** manipulating user input in such a way that, when processed by the database server, it will be interpreted as code, potentially providing direct access to private data.
- **Padding Oracle attacks —** altering a block-cypher cryptographic hash in such a way as to decrypt encrypted information.

Product	URL Parameter Manipulation	Form / Hidden Field Manipulation	Cookie / Session Poisoning	Cross-Site Scripting (XSS)	Directory Traversal	SQL Injection	Padding Oracle Attacks
Barracuda Networks Web Application Firewall 960	100%	100%	100%	99.77%	100%	100%	100%
Citrix NetScaler AppFirewall MPX 11520	100%	100%	100%	98.39%	100%	100%	100%
Fortinet FortiWeb 1000D	100%	100%	100%	98.96%	100%	100%	100%
F5 Big-IP ASM 10200	100%	100%	100%	99.25%	100%	100%	100%
Imperva SecureSphere x6500	100%	100%	100%	98.73%	100%	100%	100%
Sangfor M5900-F-I	100%	100%	100%	72.74%	100%	100%	100%

Figure 4 – Attack Types

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 measures. Failure of a security device to handle correctly a particular type of evasion potentially will allow an attacker to use an entire class of attacks 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 WAF product category.

Providing exploit protection results without fully factoring in evasion can be misleading. The more classes of evasion that are missed— packet fragmentation reassembly, stream segmentation, URL obfuscation and normalization —the less effective the device. For example, it is better to miss all techniques in one evasion category (say, stream segmentation) than one technique in each category, which would result in a broader attack surface. Figure 5 depicts the results of the evasion tests.

Product	Packet Fragmentation Reassembly	Stream Segmentation	URL Obfuscation and Normalization
Barracuda Networks Web Application Firewall 960	PASS	PASS	PASS
Citrix NetScaler AppFirewall MPX 11520	PASS	PASS	PASS
Fortinet FortiWeb 1000D	PASS	PASS	PASS
F5 Big-IP ASM 10200	PASS	PASS	PASS
Imperva SecureSphere x6500	PASS	PASS	PASS
Sangfor M5900-F-I	PASS	PASS	PASS

Figure 5 – Evasions

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 DUT failing open for any reason, this will result in a FAIL.

Product	Blocking under Extended Attack	Passing Legitimate Traffic under Extended Attack	Protocol Fuzzing & Mutation – Detection Ports	Protocol Fuzzing & Mutation – Management Port
Barracuda Networks Web Application Firewall 960	PASS	PASS	PASS	PASS
Citrix NetScaler AppFirewall MPX 11520	PASS	PASS	PASS	PASS
Fortinet FortiWeb 1000D	PASS	PASS	PASS	PASS
F5 Big-IP ASM 10200	PASS	PASS	PASS	PASS
Imperva SecureSphere x6500	PASS	PASS	PASS	PASS
Sangfor M5900-F-I	PASS	PASS	PASS	PASS

Figure 6 – Stability and Reliability (I)

Product	Power Fail	Redundancy	Persistence of Data	Stability and Reliability
Barracuda Networks Web Application Firewall 960	PASS	YES	PASS	PASS
Citrix NetScaler AppFirewall MPX 11520	PASS	YES	PASS	PASS
Fortinet FortiWeb 1000D	PASS	YES	PASS	PASS
F5 Big-IP ASM 10200	PASS	YES	PASS	PASS
Imperva SecureSphere x6500	PASS	YES	PASS	PASS
Sangfor M5900-F-I	PASS	YES	PASS	PASS

Figure 7 – 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 block rate. Figure 8 depicts the *security effectiveness* of each device.

Product	Block Rate	Evasions	Stability and Reliability	Security Effectiveness
Barracuda Networks Web Application Firewall 960	99.97%	100%	100%	99.97%
Citrix NetScaler AppFirewall MPX 11520	99.77%	100%	100%	99.77%
Fortinet FortiWeb 1000D	99.85%	100%	100%	99.85%
F5 Big-IP ASM 10200	99.89%	100%	100%	99.89%
Imperva SecureSphere x6500	99.82%	100%	100%	99.82%
Sangfor M5900-F-I	96.11%	100%	100%	96.11%

Figure 8 – Security Effectiveness

Test Methodology

Web Application Firewall: v6.2

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.