WEB APPLICATION FIREWALL COMPARATIVE ANALYSIS

Security Value Map™ (SVM)

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

Empirical data from individual Product Analysis Reports (PARs) and Comparative Analysis Reports (CARs) is used to create the unique Security Value Map™ (SVM). The SVM illustrates the relative value of security investment options by mapping *security effectiveness* and value (*TCO per protected - connections per second (CPS))* of tested product configurations.

The SVM provides an aggregated view of the detailed findings from NSS Labs' group tests. Individual PARs are available for every product tested. CARs provide detailed comparisons across all tested products in the areas of:

- Security
- Performance
- Total cost of ownership (TCO)

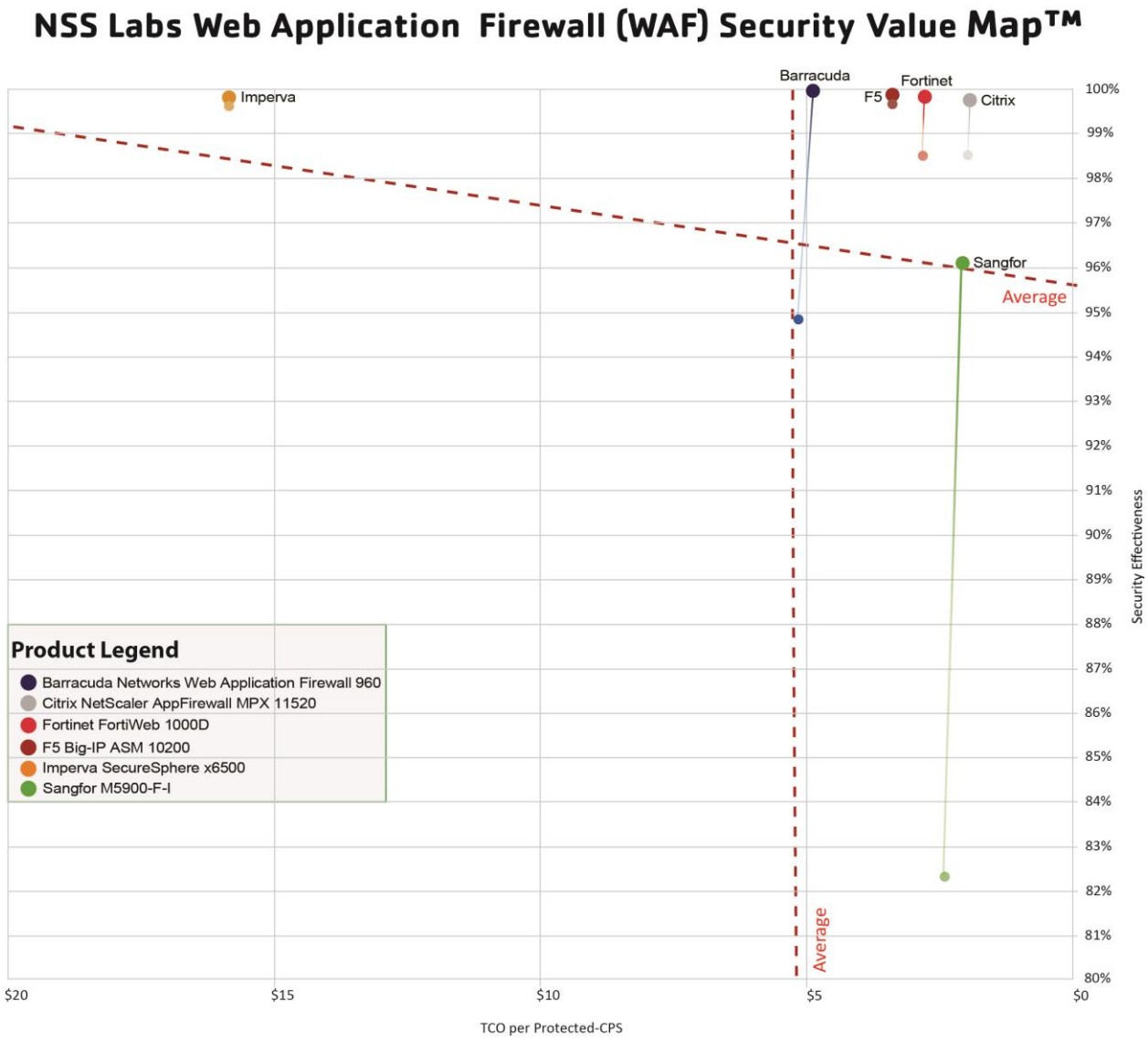

Figure 1 – NSS Labs Security Value Map (SVM) for Web Application Firewall (WAF)

Key Findings

- Overall *security effectiveness* varied between 96.11% and 99.97%, with 5 of the 6 tested products achieving greater than 99.75%.
- *TCO per protected-CPS* varied from US $1.93 to US $15.85, with most tested devices costing below US $5.00 *per protected-CPS*.
- Average *value* (*TCO per protected-CPS*) was US $5.15 – 5 devices were rated as above average *value* and 1 were below average.
- *NSS-tested capacity* ranged from 12,640 CPS to 76,616 CPS.

Product Rating

The overall rating in figure 2 is determined based on which SVM quadrant the product falls within – ***Recommended*** (top right), ***Neutral*** (top left or bottom right), or ***Caution*** (bottom left). For more information on how the SVM is constructed, please see the "*How to Read the SVM"* section in this document.

Product	Security Effectiveness	Value (TCO per Protected-CPS)	Overall Rating
Barracuda Networks Web Application Firewall 960	99.97%	$4.88	Recommended
Citrix NetScaler AppFirewall MPX 11520	99.77%	$1.93	Recommended
Fortinet FortiWeb 1000D	99.85%	$2.77	Recommended
F5 Big-IP ASM 10200	99.89%	$3.38	Recommended
Imperva SecureSphere x6500	99.82%	$15.85	Neutral
Sangfor M5900-F-I	96.11%	$2.07	Recommended

Figure 2 – NSS Labs Recommendations for Web Application Firewall (WAF)

The NSS Labs WAF group test reveals that many solutions in the marketplace are reasonably effective at their roles, though there are degrees of efficacy. In the SVM for WAF, each vendor is represented by two dots. The upper dot reflects the product's optimum security configuration and capability when properly tuned and deployed for the environment and applications. The lower is when protections are disabled in order to eliminate false-positives, which reduces the effective security of the device.

This report is part of a series of CARs on security, performance, TCO and SVM. In addition, NSS clients have access to an *SVM Toolkit™* that allows for the incorporation of organization-specific costs and requirements to create a completely customized SVM. For more information, please visit http://www.nsslabs.com.

Table of Contents:

Table of Figures

How to Read the SVM

The SVM depicts the value of a typical deployment of four (4) devices plus one (1) central management unit (and where necessary, a log aggregation, and/or event management unit), to provide a more accurate reflection of cost than if only a single WAF device were depicted. An example SVM is shown in figure 3.

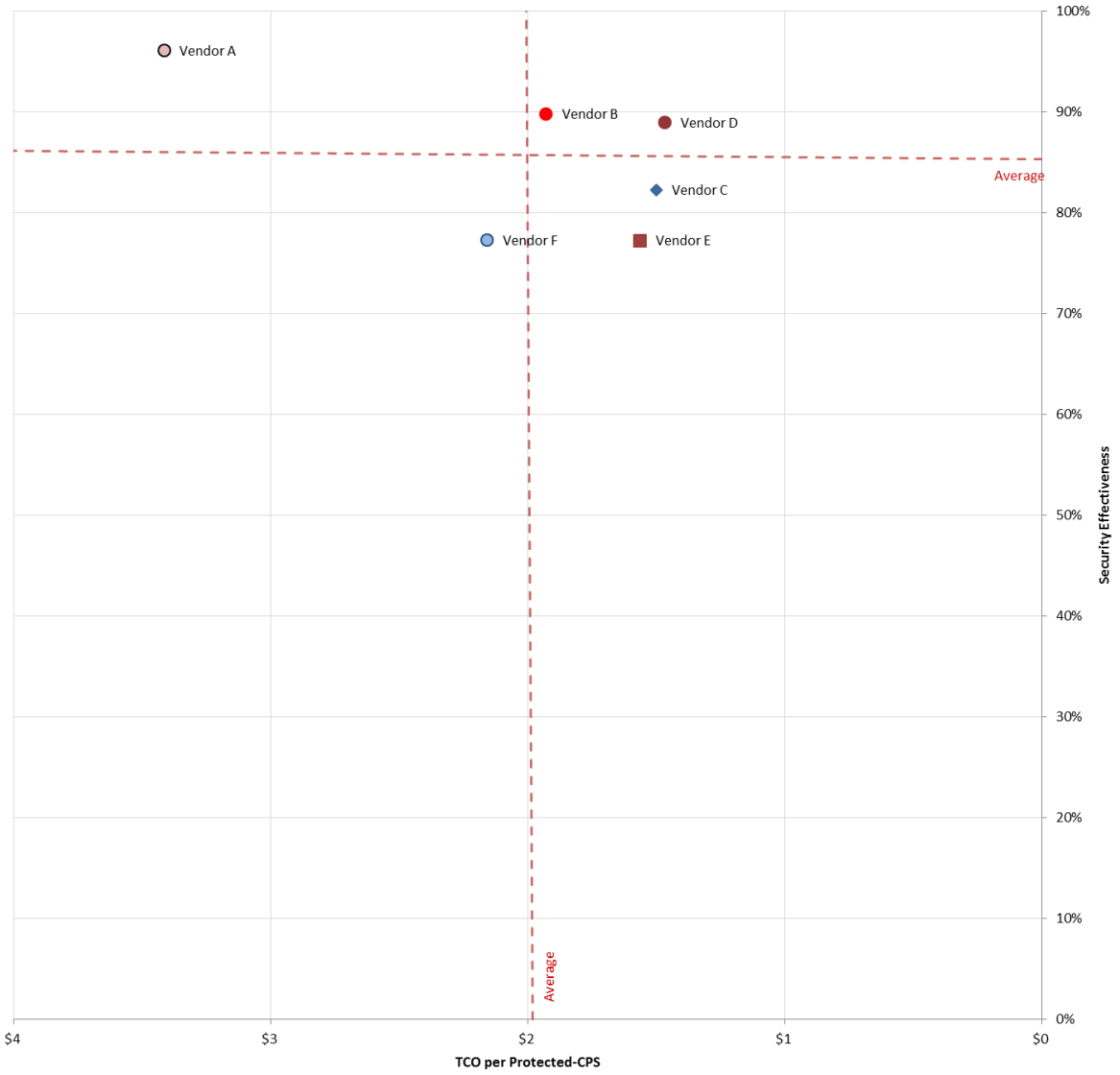

Figure 3 – Example SVM

The x-axis charts the *TCO per protected-CPS*, a metric that incorporates the 3-Year TCO with the *NSS-tested capacity* to provide a data point by which to compare the actual value of each product tested. The terms *TCO per protected-CPS* and *value* are used interchangeably throughout this report and throughout the CARs.

The y-axis charts the security effectiveness as determined in the *security effectiveness* tests. Devices that are missing critical security capabilities will have a reduced score on this axis.

Mapping the data points against the *security effectiveness* and *TCO per protected-CPS* results in four quadrants on the SVM.

- **Products that map farther up and to the right are recommended.** The upper-right quadrant contains those products that are in the ***Recommended*** category for both *security effectiveness* and *TCO per protected-CPS*. These products provide a high level of detection and value for money.
- **Products that map farther down and to the left should be used with caution**. The lower left quadrant would comprise the ***Caution*** category; these products offer limited value for money given the 3-year TCO and measured *security effectiveness* rating.
- The remaining two quadrants comprise the ***Neutral*** category. Products that fall into this category may still be worthy of a place on an organization's short list based on its specific requirements.

For example, products in the upper-left quadrant score as *above average* for *security effectiveness*, but below average for *value* (*TCO per protected-CPS)*. These products would be suitable for environments requiring a high level of detection, albeit at a higher than average cost.

Conversely, products in the lower-right quadrant score as below average for *security effectiveness*, but above average for *value* (*TCO per protected-CPS)*. These products would be suitable for environments where budget is paramount, and a slightly lower level of detection is acceptable in exchange for a lower TCO..

In all cases, the SVM should only be a starting point. NSS clients have access to the *SVM Toolkit*, which allows for the incorporation of organization-specific costs and requirements to create a completely customized SVM. Furthermore, the option is available to schedule an inquiry with NSS analysts.

Analysis

Analysis is divided into three categories based on the position of each product in the SVM: ***Recommended***, ***Neutral***, and ***Caution***. Each of the tested products will fall into only one category, and vendors are listed alphabetically within each section.

Recommended

Citrix NetScaler AppFirewall MPX 11520

Key Findings:

- Using a tuned policy, the Citrix NetScaler AppFirewall MPX 11520 blocked 99.77% of WAF attacks.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The NetScaler AppFirewall MPX 11520 presented a 0.349% false positive rate.
- The NetScaler AppFirewall MPX 11520 is rated by NSS at 46,282 connections per second (CPS), which is higher than the vendor-claimed performance. This is a minimum rating using one transaction per connection. Citrix rates this device at 6.5 Gbps, which would be 32,500 CPS at 21KB object size. NSS-tested capacity is an average of all of the HTTP response-based capacity tests.

Fortinet FortiWeb 1000D

Key Findings:

- Using a tuned policy, the Fortinet FortiWeb 1000D blocked 99.85% of WAF attacks.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The FortiWeb 1000D presented a 0.366% false positive rate.
- The FortiWeb 1000D is rated by NSS at 15,865 connections per second (CPS), which is higher the vendor-claimed performance. This is a minimum rating using one transaction per connection. Fortinet rates this device at 750 Mbps, which would be 3,750 CPS at 21KB object size. NSS-tested capacity is an average of all of the HTTP response-based capacity tests.

F5 Big-IP ASM 10200

Key Findings:

- Using a tuned policy, the F5 Big-IP ASM 10200 blocked 99.21% of WAF attacks.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The Big-IP ASM 10200 presented a 0.124% false positive rate
- The Big-IP ASM 10200 is rated by NSS at 36,130 connections per second (CPS), which is in line with the vendor-claimed performance. This is a minimum rating using one transaction per connection. F5 rates this device at 35,000 CPS. NSS-tested capacity is an average of all of the HTTP response-based capacity tests.

Barracuda Networks Web Application Firewall 960

Key Findings:

- Using a tuned policy, the Barracuda Networks Web Application Firewall 960 blocked 99.97% of WAF attacks.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The Web Application Firewall 960 presented a 0.715% false positive rate.
- The Web Application Firewall 960 is rated by NSS at 12,640 connections per second (CPS), which is lower than the vendor-claimed performance. This is a minimum rating using one transaction per connection. Barracuda Networks rates this device at 4Gbps, which would be 20,000 CPS at 21KB object size. NSS-tested capacity is an average of all of the HTTP response-based capacity tests.

Sangfor M5900-F-I

Key Findings:

- Using a tuned policy, the Sangfor M5900-F-I blocked 96.11% of WAF attacks.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The M5900-F-I presented a 1.174% false positive rate.
- The M5900-F-I is rated by NSS at 76,616 connections per second (CPS), which is higher than the vendor-claimed performance. This is a minimum rating using one transaction per connection. Sangfor rates this device at 5 Gbps, which would be 25,000 CPS at 21KB object size. NSS-tested capacity is an average of all of the HTTP response-based capacity tests.

Neutral

Imperva SecureSphere x6500

- Using a tuned policy, the SecureSphere x6500 blocked 99.82% of WAF attacks.
- The device proved effective against all evasion techniques tested.
- The device also passed all stability and reliability tests.
- The SecureSphere x6500 presented a 0.110% false positive rate.
- The SecureSphere x6500 is rated by NSS at 13,385 connections per second (CPS), which is higher than the vendor-claimed performance. This is a minimum rating using one transaction per connection. Imperva rates this device at 2.0 Gbps, which would be 10,000 CPS at 21KB object size. NSS-tested capacity is an average of all of the HTTP response-based capacity tests.

Caution

No product received a caution rating for this group test.

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
Buliding A, Suite 200
Austin, TX 78746
info@nsslabs.com
www.nsslabs.com