DATA CENTER IPS COMPARATIVE ANALYSIS

Security Value Map (SVM)

2014 – Thomas Skybakmoen, Jason Pappalexis

Tested Products

Fortinet FortiGate 5140B, Juniper SRX 5800, McAfee NS-9300, Sourcefire 8290-2

Overview

Empirical data from the individual *Product Analysis Reports* (PAR) and *Comparative Analysis Reports* (CAR) 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-Mbps) of tested product configurations. This SVM relates to data center intrusion prevention system (IPS) offerings as tested; standard enterprise perimeter IPS products are covered in a separate report.

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
- Management
- Total cost of ownership (TCO)

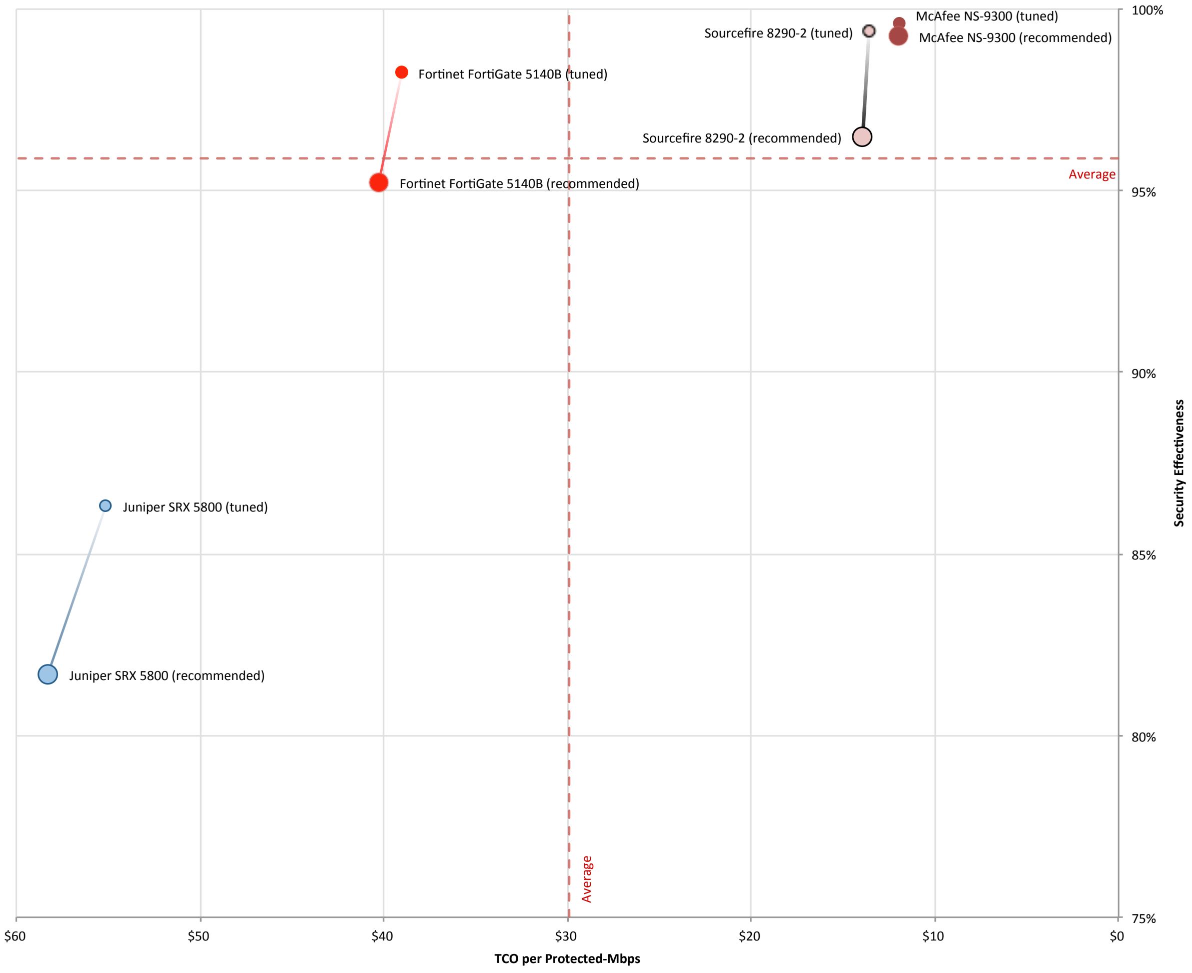

Figure 1 – NSS Labs' 2014 Security Value Map (SVM) for Data Center Intrusion Prevention Systems (IPS)

Key Findings

- NSS saw an average of 2.7% improvement in security effectiveness when comparing the recommended policy configuration to the tuned policy configuration.
- 3 of the 4 tested products achieved greater than 2.9% improvement from recommend policy configuration to tuned policy configuration.
- McAfee provided the highest security effectiveness in the test using the tuned policy configuration.
- McAfee provided the highest security effectiveness score using the recommended policy configuration ("out of the box" protection).
- TCO per Protected-Mbps varied from USD $11.94 to USD $55.13 with most tested devices costing below USD $40 per Protected-Mbps using tuned policy configuration.
- NSS-Tested Throughput ranged from 31 Gbps to 136 Gbps using tuned policy configuration.
- Average Security Effectiveness rating was 95.9% using tuned policy configuration – 3 devices were rated as above average security effectiveness, 1 was below average.
- Average Value (TCO per Protected-Mbps) was $29.91 using tuned policy configuration – 2 devices were rated as above average value and 2 were below average.
- The NSS management audit found all products to fulfill the enterprise requirement for centralized management capabilities. For more details, please see the *Management Comparative Analysis CAR*.
- The Juniper Networks SRX series are not designed or recommended by Juniper for standalone IPS deployment. They are designed for integrated Firewall + IPS deployments.

Product Rating

The *Overall Rating* in the following table 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 *"How To Read The SVM"* section in this document. Note that the position is based on the *tuned* settings, since it is assumed that data center devices will always be tuned.

Product	Security Effectiveness		Value (TCO per Protected-Mbps)		Overall Rating
Fortinet FortiGate 5140B	98.2%	Above Average	$39.02	Below Average	Neutral
Juniper SRX 5800	86.3%	Below Average	$55.13	Below Average	Caution
McAfee NS-9300	99.6%	Above Average	$11.94	Above Average	Recommended
Sourcefire 8290-2	99.4%	Above Average	$13.55	Above Average	Recommended

Figure 2 – NSS Labs' 2014 Recommendations for Data Center Intrusion Prevention Systems (IPS)

This report is part of a series of Comparative Analysis Reports (CAR) on security, performance, management, total cost of ownership (TCO) and Security Value Map (SVM). In addition, a SVM Toolkit is available to NSS clients that allows for the incorporation of organization-specific costs and requirements to create a completely customized SVM. For more information, please visit 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 a central management unit (and where necessary, a log aggregation, and/or event management unit), to provide a more accurate reflection of cost versus that of a single IPS device. The *Management CAR* outlines the pricing and license structure required for the modeled management infrastructure. An example SVM is shown in Figure 3.

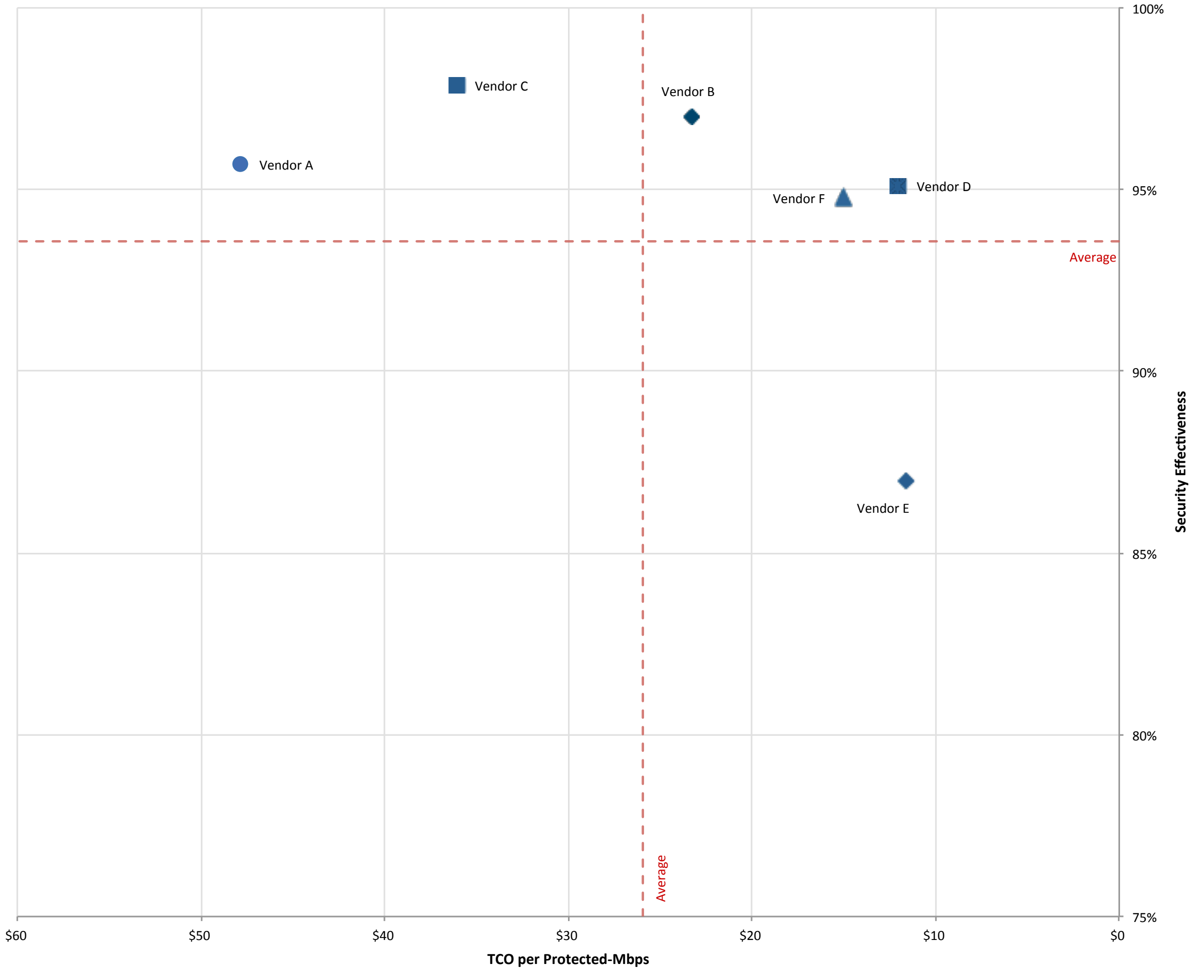

Figure 3 – Example SVM

The x-axis charts the *TCO per Protected-Mbps*, a metric that incorporates the 3-Year TCO with measured throughput to provide a single result that can be used to compare the actual *Value* of each product tested. The terms *TCO per Protected-Mbps* and *Value* are used interchangeably throughout these reports.

The y-axis charts the security effectiveness as measured via 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-Mbps* results in four quadrants on the SVM.

- **Farther up and to the right is recommended by NSS.** The upper-right quadrant contains those products that are in the ***Recommended*** category for both *security effectiveness* and *TCO per Protected-Mbps*. These products provide a very high level of detection and value for money.
- **Farther down and to the left should be used with caution**. The lower left quadrant would comprise the NSS ***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 NSS ***Neutral*** category. These products 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-Mbps)*. 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-Mbps)*. 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 cost of ownership.

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 call (or a written response) with the analysts involved in the actual testing and report production.

Analysis

The 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

McAfee NS-9300

Key Findings:

- Using a tuned policy, the NS-9300 blocked 99.6% of exploits. The device proved effective against all evasion techniques tested. The device also passed all stability and reliability tests.
- The McAfee NS-9300 is rated by NSS at 47,533 Mbps, which is higher than the vendor-claimed performance (McAfee rates this device at 40 Gbps).
- Network Security Manager (NSM) v8.0.5 fulfills enterprise requirements in areas such as policy inheritance, policy association, and the ability to view differences between policy versions.
- Built-in reporting is available with default templates per product type, access to saved reports, and some customization capabilities.
- NSM supports high availability as well as independent backup and restore of configuration.
- The console still has some dependence on Java clients, which results in additional latency depending on the features used. This could be a factor for some organizations. McAfee is incrementally removing java dependencies from the web interface.

Sourcefire 8290-2

Key Findings:

- Using a tuned policy, the 8290-2 blocked 99.4% of exploits. The device proved effective against all evasion techniques tested. The device also passed all stability and reliability tests.
- The Sourcefire 8290-2 is rated by NSS at 136,033 Mbps, which is higher than the vendor-claimed performance (Sourcefire rates this device at 80 Gbps).
- Sourcefire Defense Center 3500 v5.2 fulfills enterprise requirements in areas such as policy inheritance, policy association, and the ability to view differences between policy versions.
- Built-in reporting is available with default templates per product type, access to saved reports, and customization capabilities.
- Integration with third-party technologies provides the extensibility required for enterprise customers.
- Defense Center supports high availability as well as independent backup and restore of configuration.

Neutral

Fortinet FortiGate 5140B

Key Findings:

- Using a tuned policy, the Fortigate 5140B blocked 98.4% of exploits. The device proved effective against all evasion techniques tested. The device also passed all stability and reliability tests.
- The Fortinet Fortigate 5140B is rated by NSS at 59,340 Mbps, which is lower than the vendor-claimed performance (Fortinet rates this device at 120 Gbps).
- Fortinet FortiManager v5.0.5 fulfills enterprise requirements in areas such as policy inheritance, policy association, and the ability to view differences between policy versions.
- Built-in reporting is provided. Multiple default templates are available, with some customization possible.
- FortiManager supports high availability as well as independent backup and restore of configuration and databases.
- The FortiManager opening view is the *Device Manager* tab that provides visibility into system health, policy information, and license status rather than security alerts. Primary focus is on infrastructure instead of security, and this may or may not fit all organizational needs.

Caution

Juniper SRX 5800

Key Findings:

- The Juniper Networks SRX series are not designed or recommended by Juniper for standalone IPS deployment. They are designed for integrated Firewall + IPS deployments.
- Using a tuned policy, the SRX 5800 blocked 86.3% of exploits. The device proved effective against all evasion techniques tested. The device also passed all stability and reliability tests.
- The Juniper SRX 5800 is rated by NSS at 31,625 Mbps, which is lower than the vendor-claimed performance (Juniper rates this device at 40 Gbps).
- Juniper Junos Space Security Director v13.1 & Secure Analytics fulfills enterprise requirements for policy inheritance, policy association, and the ability to view differences in applied policy versions. However, the CMS lacks the ability to view policy and/or triggered rule directly from a security event with a single click or menu option. This can increase the time required to determine the root cause of a security event and will increase TCO for some environments.
- Reporting is available with some default templates, access to saved reports, and some customizability for new reports. Since Junos Space is a network-centric tool, reports can include components other than security.
- High availability, backup and restore and redundancy features are available. Junos Space operates as a node on the existing Juniper network fabric, and, as such, a wide range of disaster recovery resources is available. A system snapshot is required to allow system state rollback as needed.
- Secure Analytics is required for security event logging/reporting, which makes Juniper a “swivel chair” management system, whereby the administrator is required to move between systems to obtain full system visibility. Improved integration between the two systems would result in lower TCO.

Test Methodology

Methodology Version: Data Center IPS Test Methodology v1.1.1

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
+1 (512) 961-5300
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 at +1 (512) 961-5300 or sales@nsslabs.com.

Please note that access to or use of this report is conditioned on the following:

1. The information in this report is subject to change by NSS Labs without notice.

2. The information in this report is believed by NSS Labs to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at the reader's sole risk. NSS Labs is not liable or responsible for any damages, losses, or expenses arising from any error or omission in this report.

3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY NSS LABS. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY NSS LABS. IN NO EVENT SHALL NSS LABS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL 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 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 the reader's 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.