DATA CENTER IPS COMPARATIVE ANALYSIS

Total Cost of Ownership (TCO)

2014 – Thomas Skybakmoen, Jason Pappalexis

Tested Products

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

Overview

The implementation of intrusion prevention system (IPS) solutions can be a complex process, with multiple factors affecting the overall cost of deployment, maintenance, and upkeep. These should be considered over the course of the useful life of the solution, and include:

1. Acquisition costs for IPS devices and central management system
2. Fees paid to the vendor for annual maintenance, support and signature updates
3. Labor costs for installation, maintenance and upkeep

No two network security products deliver the same security effectiveness or throughput, making precise comparisons extremely difficult. In order to capture the relative value of devices on the market and facilitate such comparisons, NSS Labs has developed a unique metric to enable value-based comparisons: *TCO per protected megabit per second* (see Figure 1).

By using total cost of ownership (TCO) instead of purchase price, it is possible to factor in management of the device via labor costs associated with product installation, maintenance, upkeep, and tuning. This metric is used extensively in the following sections to evaluate cost of security, throughput, and 3-year TCO. The benefit from this analysis is that, within a given performance range, it can provide some insight as to whether a product is priced above or below the majority of its competitors. A high price could indicate a premium based upon protection offered, brand recognition, level of customer service, or a price penalty for an underperforming product.

***Security Effectiveness** = Exploit Block Rate[1] x Evasion x Stability & Reliability*
***TCO per Protected Megabit per Second** = TCO/(Security Effectiveness * NSS-Tested Throughput)*

Figure 1 – Security Effectiveness Formula

Product	NSS-Tested Throughput (Mbps)	Purchase Price	Security Effectiveness	3-Year TCO	TCO per Protected-Mbps
Fortinet FortiGate 5140B	59,340	$4,153,094	98.2%	$9,098,576	$39
Juniper SRX 5800	31,625	$5,145,000	86.3%	$6,020,490	$55
McAfee NS-9300	47,533	$1,261,990	99.6%	$2,262,034	$12
Sourcefire 8290-2	136,033	$5,091,918	99.4%	$7,328,304	$14

Figure 2 – Total Cost of Ownership per Protected-Mbps

For the purpose of this analysis, NSS developed an enterprise use case with one (1) central management system and four (4) devices deployed across multiple remote locations. Since configuration is performed via central management, the device cost reflects only initial setup and upkeep per device.

NSS' research indicates that all enterprises tune their IPS devices when deployed in the data center. Therefore, for NSS' testing of IPS 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 IPS security effectiveness and performance capabilities, based on their expected usage.

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

Table of Contents

Analysis **4**
Labor and Equipment Costs 4
Labor for Device Setup and Upkeep *4*
Labor for Central Management *5*
Equipment and Software Costs *5*
Total Cost of Ownership 6
Normalizing the Data 6
Purchase Price (Vendor-Claimed Performance) *6*
Total Cost of Ownership (Vendor-Claimed Performance) *7*
Factor in Protection *7*
Factor in Performance *8*
Total Cost of Ownership with NSS-Tested Throughput *8*
Factor in Security Effectiveness *8*
Determining Value 9
Security Effectiveness and Value *10*
Test Methodology **11**
Contact Information **11**

Table of Figures

Figure 1 – Security Effectiveness Formula *2*
Figure 2 – Total Cost of Ownership per Protected-Mbps *2*
Figure 3 – Labor per IPS Device *4*
Figure 4 – Labor Required for Central Management *5*
Figure 5 – Equipment and Software Costs *5*
Figure 6 – Year 1 Total Cost of Ownership *6*
Figure 7 – Purchase Price per Mbps (Vendor-Claimed Throughput) *6*
Figure 8 – TCO per Mbps (Vendor-Claimed Throughput) *7*
Figure 9 – Purchase Price per Protected-Mbps (Vendor-Claimed Throughput & Protection) *7*
Figure 10 – TCO per Protected-Mbps (Vendor-Claimed Throughput & Protection) *7*
Figure 11 – Vendor-Claimed vs. NSS-Tested Throughput (Mbps) *8*
Figure 12 – Purchase price per Protected-Mbps (NSS-Tested Throughput & Protection) *8*
Figure 13 – TCO per Protected-Mbps (NSS-Tested Throughput & Protection) *8*
Figure 14 – Purchase Price per Protected-Mbps (NSS-Tested Throughput & Security Effectiveness) *9*
Figure 15 – TCO per Protected-Mbps (NSS-Tested Throughput & Security Effectiveness) *9*
Figure 16 – Value based on Purchase Price *9*
Figure 17 – Value based on TCO *10*
Figure 18 – Comparison of Purchase Price to Security Effectiveness Value *10*

Analysis

Labor and Equipment Costs

IPS solutions are among the most complex products in information security discipline. 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.

This table estimates the annual labor required to maintain each device. There are three main components to be considered:

- **Installation (capital expenditure/CAPEX) –** the time required to take the device out of the box, configure it, put it into the network, apply updates and patches, perform initial tuning, and configure desired logging and reporting.
- **Upkeep (operating expenditure/OPEX)** – the time required for administration, policy handling, log handling, alert handling, monitoring, reporting, analysis, auditing & compliance, maintenance, software updates, troubleshooting, etc.
- **Tuning (operating expenditure/OPEX)** – the ongoing time required to configure the policy such that the best possible protection is applied while reducing or eliminating false alarms and false positives.

Labor for Device Setup and Upkeep

This table estimates the annual labor required to maintain each device. NSS' assumptions are based on the time that would be required by an experienced security engineer (USD $75 per hour), thus allowing NSS to hold constant the talent cost, and measure only the difference in time required for installation and upkeep.

Readers should substitute their own costs to obtain accurate TCO figures by using the *SVM Toolkit,* available to clients.

Product	Installation (Hours)	Upkeep (Hours per Year)
Fortinet FortiGate 5140B	10	8
Juniper SRX 5800	10	10
McAfee NS-9300	16	8
Sourcefire 8290-2	16	8

Figure 3 – Labor per IPS Device

Labor for Central Management

Labor costs for central management refer to day-to-day management tasks, including administration, policy handling, log handling, alert handling, monitoring, reporting, analysis, auditing & compliance, maintenance, software updates, troubleshooting, etc.

Upkeep and *Tuning* are based on the assumption that, within a typical enterprise, administrators will use some form of centralized management system to manage deployed security devices. Without central management, it would be necessary to extrapolate these hours (and thus increase costs) by multiplying them by the number of deployed devices. The variation in installation/setup and upkeep time reflects the efficiency of each management system.

Product	Installation (Hours)	Upkeep (Hours per Year)	Tuning (Hours per Year)
Fortinet FortiGate 5140B	8	8	1,300
Juniper SRX 5800	16	10	1,400
McAfee NS-9300	8	8	900
Sourcefire 8290-2	8	8	1,000

Figure 4 – Labor Required for Central Management

Equipment and Software Costs

All product costs are based on list prices as provided to NSS researchers by vendors. Actual costs to end-users may be lower depending on the negotiated discount. However, assuming all vendors will provide similar discounts, the cost ratios will remain constant.

NSS clients can use the *SVM Toolkit* to record actual negotiated prices, labor costs, and upkeep times, in order to generate their own results and customized *SVM* to compare with the data in this report. For more details on management, hardware, software, licensing, and support costs, please see the *"IPS Data Center Comparative Analysis Report – Management."*

Product	Initial Purchase Price (Hardware As Tested)	Initial Purchase Price (Enterprise Management System)	Annual Cost Of Maintenance & Support (Hardware/Software)	Annual Cost Of Maintenance & Support (Enterprise Management)	Annual Cost Of Updates (IPS/AV/etc.)
Fortinet FortiGate 5140B	$1,035,961	$9,250	$214,363	$2,990	$167,988
Juniper SRX 5800	$1,280,000	$25,000	$19,720	$4,800	$20,000
McAfee NS-9300	$310,000	$21,990	$62,000	$2,398	$0
Sourcefire 8290-2	$1,267,980	$19,998	$163,078	$2,700	$0

Figure 5 – Equipment and Software Costs

Total Cost of Ownership

TCO incorporates both CAPEX and OPEX costs over a three-year period. This includes initial acquisition and deployment costs, plus annual maintenance and update costs (software and hardware updates), and all associated labor costs. Upkeep labor includes day-to-day management, patching/updating, troubleshooting, etc.

Calculations are as follows:

Value	Description of Calculation
Year One Cost	Initial Purchase Price + Maintenance Cost + (Installation + Upkeep + Tuning) x Labor rate $/hr)
Year Two Cost	Maintenance Cost + (Upkeep + Tuning hours) x Labor rate $/hr)
Year Three Cost	Maintenance Cost + (Upkeep + Tuning hours) x Labor rate $/hr)
Three Year TCO	Year One Cost + Year Two Cost + Year Three Cost

Calculations are based on a labor rate of USD $75 per hour as well as vendor-provided pricing information. Where possible, the 24/7 maintenance and support option with 24-hour replacement is utilized, since this is the option typically selected by enterprise customers. Pricing includes an enterprise-class centralized management solution to manage up to four (4) devices. High availability is included in the cost modeling for centralized management.

Product	Purchase Price	Maintenance per Year	Year 1 Product Cost	Year 1 Labor Cost	1-Year TCO
Fortinet FortiGate 5140B	$4,153,094	$1,532,394	$5,685,488	$118,500	$5,803,988
Juniper SRX 5800	$5,145,000	$163,680	$5,308,680	$130,950	$5,439,630
McAfee NS-9300	$1,261,990	$250,398	$1,512,388	$86,550	$1,598,938
Sourcefire 8290-2	$5,091,918	$655,012	$5,746,930	$94,050	$5,840,980

Figure 6 – Year 1 Total Cost of Ownership

Normalizing the Data

There are multiple methods by which value can be determined. The benefit of this analysis is that, within a given performance range, it will provide insight as to whether a product is priced above or below the majority of its competitors. A high price could indicate a premium based on protection offered, brand recognition, level of customer service, or a cost penalty for an underperforming product.

Purchase Price (Vendor-Claimed Performance)

The most simplistic means of determining "value," but frequently misleading, is determining the price per megabit per second, based on the initial purchase price of the product and the performance claims of the vendor.

Product	Vendor-Claimed Throughput (Mbps)	Purchase Price	Purchase Price per Mbps
Fortinet FortiGate 5140B	120,000	$4,153,094	$9
Juniper SRX 5800	40,000	$5,145,000	$32
McAfee NS-9300	40,000	$1,261,990	$8
Sourcefire 8290-2	80,000	$5,091,918	$16

Figure 7 – Purchase Price per Mbps (Vendor-Claimed Throughput)

Total Cost of Ownership (Vendor-Claimed Performance)

A more sophisticated approach involves determining the price per megabit per second, based on the total cost of ownership of the product. This calculation is performed in many purchasing departments. Unfortunately, this approach is equally flawed, since it relies on the vendor-claimed performance, without independent testing, to determine the **actual** throughput of the device under real-world conditions.

Product	Vendor-Claimed Throughput (Mbps)	Purchase Price	3-Year TCO	TCO per Mbps
Fortinet FortiGate 5140B	120,000	$4,153,094	$9,098,576	$19
Juniper SRX 5800	40,000	$5,145,000	$6,020,490	$38
McAfee NS-9300	40,000	$1,261,990	$2,262,034	$14
Sourcefire 8290-2	80,000	$5,091,918	$7,328,304	$23

Figure 8 – TCO per Mbps (Vendor-Claimed Throughput)

Factor in Protection

Determining value purely upon TCO and throughput is acceptable when dealing with a pure networking device. However, for security devices, protection (in the case of IPS, this is represented by *Exploit Block Rate*) must also be factored into the equation. This table determines the *protected* price per megabit per second based on purchase price, vendor-claimed performance, and exploit block rate as tested.

Product	Vendor-Claimed Throughput (Mbps)	Purchase Price	Exploit Block Rate	Purchase Price per Protected-Mbps
Fortinet FortiGate 5140B	120,000	$4,153,094	98.2%	$9
Juniper SRX 5800	40,000	$5,145,000	86.3%	$37
McAfee NS-9300	40,000	$1,261,990	99.6%	$8
Sourcefire 8290-2	80,000	$5,091,918	99.4%	$16

Figure 9 – Purchase Price per Protected-Mbps (Vendor-Claimed Throughput & Protection)

The following table determines the TCO per protected Mbps based upon the 3-year TCO, vendor-claimed performance, and exploit block rate as tested.

Product	Vendor-Claimed Throughput (Mbps)	Purchase Price	Exploit Block Rate	3-Year TCO	TCO per Protected-Mbps
Fortinet FortiGate 5140B	120,000	$4,153,094	98.2%	$9,098,576	$19
Juniper SRX 5800	40,000	$5,145,000	86.3%	$6,020,490	$44
McAfee NS-9300	40,000	$1,261,990	99.6%	$2,262,034	$14
Sourcefire 8290-2	80,000	$5,091,918	99.4%	$7,328,304	$23

Figure 10 – TCO per Protected-Mbps (Vendor-Claimed Throughput & Protection)

Factor in Performance

Vendor performance claims are frequently exaggerated in marketing materials, or simply fail to take into account real-world deployment conditions. Knowing this, many enterprise IT professionals will over-purchase based on performance claims to ensure adequate performance headroom. Below is a chart of vendor-claimed throughput vs. NSS-Tested Throughput.

Product	Vendor-Claimed Throughput (Mbps)	NSS-Tested Throughput (Mbps)	% Delta
Fortinet FortiGate 5140B	120,000	59,340	-51%
Juniper SRX 5800	40,000	31,625	-21%
McAfee NS-9300	40,000	47,533	19%
Sourcefire 8290-2	80,000	136,033	70%

Figure 11 – Vendor-Claimed vs. NSS-Tested Throughput (Mbps)

Total Cost of Ownership with NSS-Tested Throughput

Because there are often significant deltas between vendor-claimed and NSS-tested performance figures, the following tables factor in the throughput as tested by NSS engineers. This begins to provide an indication of the real cost of a device based on real-world performance.

The following table determines the price per protected megabit based on the purchase price of the product, exploit block rate as tested, and the actual performance based on NSS test results.

Product	Vendor-Claimed Throughput (Mbps)	NSS-Tested Throughput (Mbps)	Purchase Price	Exploit Block Rate	Purchase Price per Protected-Mbps
Fortinet FortiGate 5140B	120,000	59,340	$4,153,094	98.2%	$18
Juniper SRX 5800	40,000	31,625	$5,145,000	86.3%	$47
McAfee NS-9300	40,000	47,533	$1,261,990	99.6%	$7
Sourcefire 8290-2	80,000	136,033	$5,091,918	99.4%	$9

Figure 12 – Purchase price per Protected-Mbps (NSS-Tested Throughput & Protection)

The following table shows the TCO per protected-Mbps based upon the 3-year TCO, exploit block rate as tested, and actual performance based upon NSS test results.

Product	Vendor-Claimed Throughput (Mbps)	NSS-Tested Throughput (Mbps)	Purchase Price	Exploit Block Rate	3-Year TCO	TCO per Protected-Mbps
Fortinet FortiGate 5140B	120,000	59,340	$4,153,094	98.2%	$9,098,576	$39
Juniper SRX 5800	40,000	31,625	$5,145,000	86.3%	$6,020,490	$55
McAfee NS-9300	40,000	47,533	$1,261,990	99.6%	$2,262,034	$12
Sourcefire 8290-2	80,000	136,033	$5,091,918	99.4%	$7,328,304	$14

Figure 13 – TCO per Protected-Mbps (NSS-Tested Throughput & Protection)

Factor in Security Effectiveness

The security effectiveness of a device factors in exploits, evasions, and stability & reliability scores (see Figure 1 – *Security Effectiveness Formula* Each of these factors can have a serious impact on security protection or business continuity when deploying in-line security devices.

The following table determines the price per protected megabit based on the purchase price of the product, actual performance based upon NSS test results, and the security effectiveness rating (calculated per Figure 1 – *Security Effectiveness Formula).*

Product	Vendor-Claimed Throughput (Mbps)	NSS-Tested Throughput (Mbps)	Purchase Price	Security Effectiveness	Purchase Price per Protected-Mbps
Fortinet FortiGate 5140B	120,000	59,340	$4,153,094	98.2%	$18
Juniper SRX 5800	40,000	31,625	$5,145,000	86.3%	$47
McAfee NS-9300	40,000	47,533	$1,261,990	99.6%	$7
Sourcefire 8290-2	80,000	136,033	$5,091,918	99.4%	$9

Figure 14 – Purchase Price per Protected-Mbps (NSS-Tested Throughput & Security Effectiveness)

The following table shows the TCO per protected-Mbps based upon the 3-year TCO, actual performance based upon NSS test results, and the security effectiveness rating.

Product	Vendor-Claimed Throughput (Mbps)	NSS-Tested Throughput (Mbps)	Purchase Price	Security Effectiveness	3-Year TCO	TCO per Protected-Mbps
Fortinet FortiGate 5140B	120,000	59,340	$4,153,094	98.2%	$9,098,576	$39
Juniper SRX 5800	40,000	31,625	$5,145,000	86.3%	$6,020,490	$55
McAfee NS-9300	40,000	47,533	$1,261,990	99.6%	$2,262,034	$12
Sourcefire 8290-2	80,000	136,033	$5,091,918	99.4%	$7,328,304	$14

Figure 15 – TCO per Protected-Mbps (NSS-Tested Throughput & Security Effectiveness)

Determining Value

The following tables demonstrate the way in which the actual value of a product can change dramatically as tested performance and security effectiveness are factored in.

Product	Vendor-Claimed Throughput (Mbps)		NSS-Tested Throughput (Mbps)	NSS-Tested Throughput + Security Effectiveness
	Purchase Price per Mbps	Price per Protected-Mbps	Price per Protected-Mbps	Price per Protected-Mbps
Fortinet FortiGate 5140B	$9	$9	$18	$18
Juniper SRX 5800	$32	$37	$47	$47
McAfee NS-9300	$8	$8	$7	$7
Sourcefire 8290-2	$16	$16	$9	$9

Figure 16 – Value based on Purchase Price

Product	Vendor-Claimed Throughput (Mbps)		NSS-Tested Throughput (Mbps)	NSS-Tested Throughput + Security Effectiveness
	TCO per Mbps	TCO per Protected-Mbps	TCO per Protected-Mbps	TCO per Protected-Mbps
Fortinet FortiGate 5140B	$19	$19	$39	$39
Juniper SRX 5800	$38	$44	$55	$55
McAfee NS-9300	$14	$14	$12	$12
Sourcefire 8290-2	$23	$23	$14	$14

Figure 17 – Value based on TCO

Security Effectiveness and Value

This compares the vendor-claimed value metric with the metric generated from NSS test results. For example, *Purchase Price per Vendor-Claimed Performance* vs. *Purchase Price per Tested Performance with Security Effectiveness.*

Product	Vendor-Claimed Throughput (Mbps)	NSS-Tested Throughput + Security Effectiveness				
	Purchase Price per Mbps	Purchase Price per Protected-Mbps	Purchase Price	Security Effectiveness Value	Delta	% Delta
Fortinet FortiGate 5140B	$9	$18	$4,153,094	$3,174,513	($978,581)	-24%
Juniper SRX 5800	$32	$47	$5,145,000	$1,486,579	($3,658,421)	-71%
McAfee NS-9300	$8	$7	$1,261,990	$2,578,623	$1,316,633	104%
Sourcefire 8290-2	$16	$9	$5,091,918	$7,361,047	$2,269,129	45%

Figure 18 – Comparison of Purchase Price to Security Effectiveness Value

The *Security Effectiveness Value* indicates whether a product is underpriced, overpriced, or priced accurately depending on the measured performance and overall security effectiveness.

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
Building A, Suite 200
Austin, TX 78746
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com