BREACH DETECTION SYSTEMS TEST REPORT

Fortinet FortiSandbox-2000E v.FSA 2.4.1 & FortiClient (ATP Agent)

v.5.6.0.1075

OCTOBER 19, 2017

Authors – Dipti Ghimire, James Hasty

Overview

NSS Labs performed an independent test of the Fortinet FortiSandbox-2000E v.FSA 2.4.1 & FortiClient (ATP Agent) v.5.6.0.1075. The product was subjected to thorough testing at the NSS facility in Austin, Texas, based on the Breach Detection Systems (BDS) Test Methodology v4.0 available at www.nsslabs.com. This test was conducted free of charge and NSS did not receive any compensation in return for Fortinet's participation.

While the companion Comparative Reports on security, performance, and total cost of ownership (TCO) will provide information about all tested products, this Test Report provides detailed information not available elsewhere.

As part of the initial BDS test setup, devices are tuned as deemed necessary by the vendor. 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 device in a live network environment. Figure 1 presents the overall results of the tests.

Product				Breach Detection Rate[1]	NSS-Tested Throughput		3-Year TCO (US$)
Fortinet FortiSandbox-2000E v.FSA 2.4.1 & FortiClient (ATP Agent) v.5.6.0.1075				99.0%	8,667 Mbps		$130,405
False Positives	Drive-by Exploits	Social Exploits	HTTP Malware	SMTP Malware	Off-Line Infections	Evasions	Stability & Reliability
0.06%	95.8%	93.3%	100.0%	100.0%	93.3%	99.38%	PASS

Figure 1 – Overall Test Results

The Fortinet FortiSandbox-2000E & FortiClient (ATP Agent) received a breach detection rating of 99.0%. The Fortinet FortiSandbox-2000E & FortiClient (ATP Agent) failed to detect 2% of the Sandbox Evasions. The product passed all stability and reliability tests.

The Fortinet FortiSandbox-2000E was tested and rated by NSS at 8,667 Mbps. *NSS-Tested Throughput* is calculated as an average of the "real-world" protocol mixes (Enterprise Perimeter and Financial), and the 21 KB HTTP response-based tests.

[1] Detection rate is defined as the average percentage of malware and exploits detected under test.

Table of Contents

Table of Figures

Security Effectiveness

This section aims to verify that the product can detect and log breaches and attempted breaches accurately. All tests in this section are completed with no background network load.

This test utilizes threats and attack methods that exist in the wild and that are currently being used by cybercriminals and other threat actors. For live testing, NSS employs a unique live test harness, the CAWS Continuous Security Validation Platform, to measure how well security products protect against "drive-by" exploits that target client applications.

The CAWS Continuous Security Validation Platform captures thousands of suspicious URLs per day from threat data generated from NSS and its customers, as well as data from open-source and commercial threat feeds. This list of URLs is optimized and assigned to victim machines, each of which has a unique combination of operating system (including service pack/patch level), browser, and client application. For details on live testing, please refer to the latest Security Stack (Network) Test Methodology, which can be found at www.nsslabs.com.

The ability of the product to detect and report successful infections in a timely manner is critical to maintaining the security and functionality of the monitored network. Infection and transmission of malware should be reported quickly and accurately, giving administrators the opportunity to contain the infection and minimize impact on the network.

As response time is critical in halting the damage caused by malware infections, the system under test should be able to detect known samples, or analyze unknown samples, and report on them within 24 hours of initial infection and command and control (C&C) callback. Any system that does not alert on an attack, infection, or C&C callback within the detection window will not receive credit for the detection.

The following use cases may be examined to determine if the system can identify a security risk within each scenario:

- **Web-based malware attacks that rely on social engineering** – The user is deceived into clicking a malicious link to download and execute malware.
- **Web-based exploits** – Also known as "drive-by downloads," these occur when the user is infected merely by visiting a web page that hosts malicious code.
- **Socially engineered malware delivered via non-HTTP traffic** – Malware is delivered by other common means such as email, a cloaked executable (.jpeg, .exe, .zip), FTP, or an infected USB drive.
- **Blended exploits** – Also known as "doc-jacking," these are typically delivered via common documents, such as Microsoft Word documents or Excel spreadsheets, containing exploits. These exploits are typically delivered via network protocols.
- **Offline infections** – Remote users with mobile devices can become infected while outside the protection of the corporate network security. Once infected devices are reattached to the corporate network, the infection can spread.

False Positives

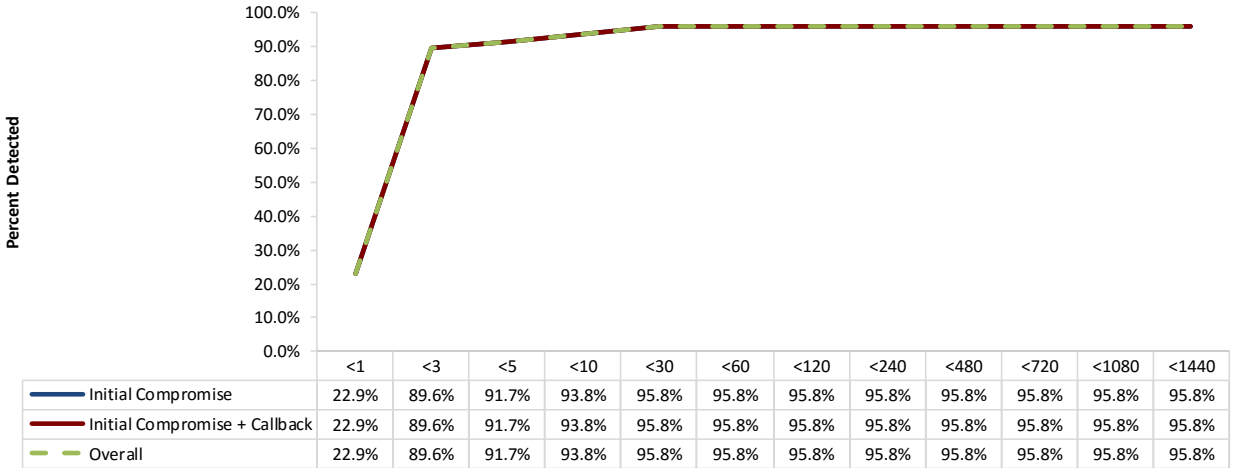
The ability of the BDS to identify legitimate traffic while maintaining detection of threats and breaches is as important as its ability to detect malicious content. This test includes a varied sample of legitimate application traffic that may be falsely identified as malicious (also known as false positives).

Figure 2 depicts the percentage of non-malicious traffic mistakenly identified as malicious. A lower score is better. The Fortinet FortiSandbox-2000E & FortiClient (ATP Agent) demonstrated a false positive rate of 0.06%.

Figure 2 – False Positive Rate

Malware Delivered by Drive-by Exploits

Figure 3 depicts malware delivered using drive-by exploits. Drive-by exploits are defined as malicious software designed to take advantage of existing deficiencies in hardware or software systems, such as vulnerabilities or bugs. Over the course of the test, the Fortinet FortiSandbox-2000E & FortiClient (ATP Agent) detected 95.8% of drive-by exploits on initial compromise and 95.8% on callback, resulting in an overall detection rate of 95.8%. Figure 3 provides a histogram of detection over time. Earlier detection is better.

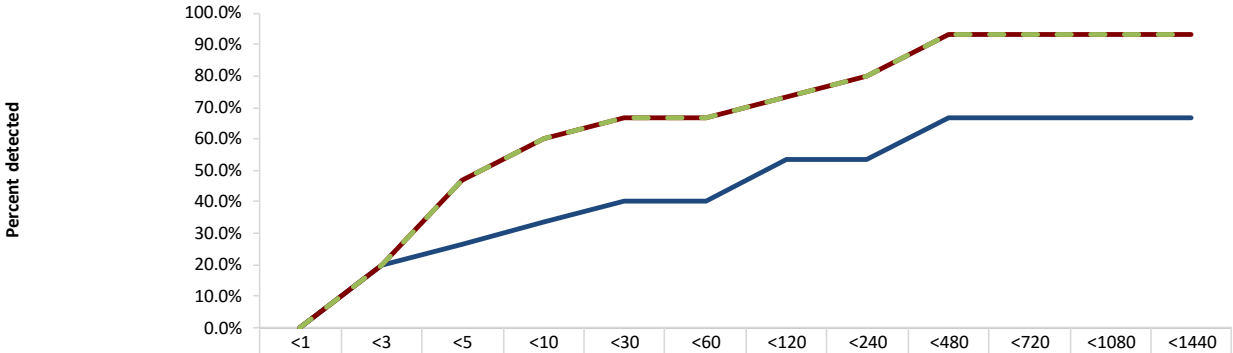


	<1	<3	<5	<10	<30	<60	<120	<240	<480	<720	<1080	<1440
Initial Compromise	22.9%	89.6%	91.7%	93.8%	95.8%	95.8%	95.8%	95.8%	95.8%	95.8%	95.8%	95.8%
Initial Compromise + Callback	22.9%	89.6%	91.7%	93.8%	95.8%	95.8%	95.8%	95.8%	95.8%	95.8%	95.8%	95.8%
Overall	22.9%	89.6%	91.7%	93.8%	95.8%	95.8%	95.8%	95.8%	95.8%	95.8%	95.8%	95.8%

Figure 3 – Malware Delivered by Drive-by Exploits: Detection over Time (Minutes)

Malware Delivered by Social Exploits

Figure 4 depicts malware delivered using social exploits. Social exploits are defined as malicious software designed to take advantage of existing deficiencies in hardware or software systems, such as vulnerabilities or bugs. Over the course of the test, the Fortinet FortiSandbox-2000E & FortiClient (ATP Agent) detected 66.7% of exploits on initial compromise and 93.3% on callback, resulting in an overall detection rate of 93.3%. Figure 4 provides a histogram of detection over time. Earlier detection is better.

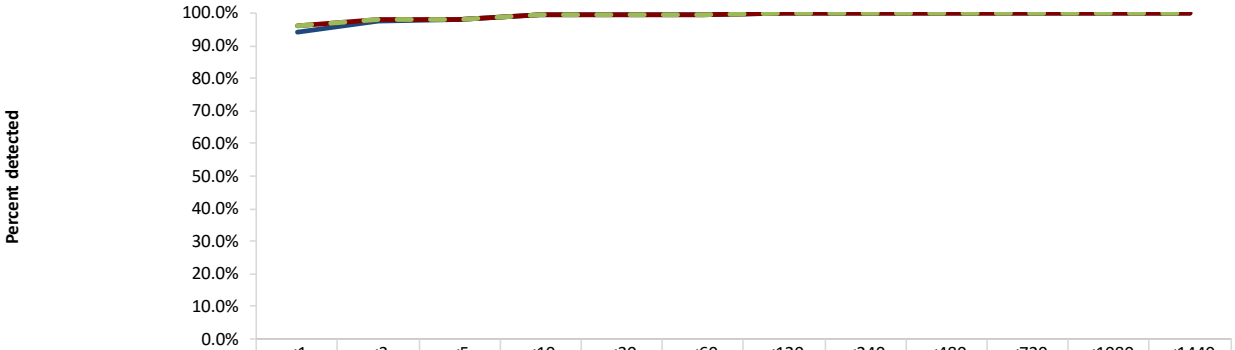


	<1	<3	<5	<10	<30	<60	<120	<240	<480	<720	<1080	<1440
Initial Compromise	0.0%	20.0%	26.7%	33.3%	40.0%	40.0%	53.3%	53.3%	66.7%	66.7%	66.7%	66.7%
Download + Callback	0.0%	20.0%	46.7%	60.0%	66.7%	66.7%	73.3%	80.0%	93.3%	93.3%	93.3%	93.3%
Overall	0.0%	20.0%	46.7%	60.0%	66.7%	66.7%	73.3%	80.0%	93.3%	93.3%	93.3%	93.3%

Figure 4 – Malware Delivered by Social Exploits: Detection over Time (Minutes)

Malware Delivered over HTTP

Figure 5 depicts malware using the HTTP protocol as its transport mechanism; that is, the malware is downloaded through a web browser. Over the course of the test, the Fortinet FortiSandbox-2000E & FortiClient (ATP Agent) detected 100% of malware on download and 100% on callback, resulting in an overall detection rate of 100%. Figure 5 provides a histogram of detection over time. Earlier detection is better.

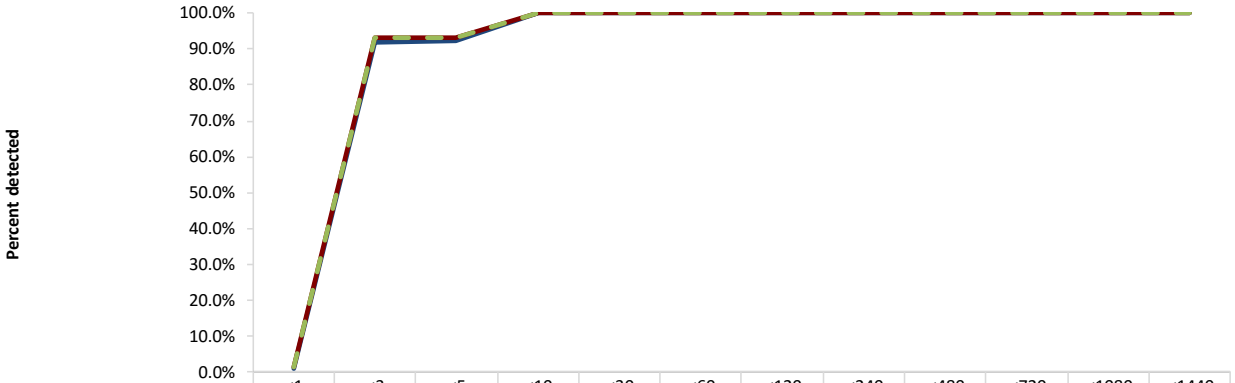


	<1	<3	<5	<10	<30	<60	<120	<240	<480	<720	<1080	<1440
Download	94.2%	97.7%	98.3%	99.4%	99.4%	99.4%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Download + Callback	95.9%	98.3%	98.3%	99.4%	99.4%	99.4%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Overall	95.9%	98.3%	98.3%	99.4%	99.4%	99.4%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Figure 5 – Malware Delivered over HTTP: Detection over Time (Minutes)

Malware Delivered over Email

Figure 6 depicts malware that uses email (SMTP) as its transport mechanism; for example, a malicious email attachment. Over the course of the test, the Fortinet FortiSandbox-2000E & FortiClient (ATP Agent) detected 100% of malware on download and 100% on callback, resulting in an overall detection rate of 100%. Figure 6 provides a histogram of detection over time. Earlier detection is better.



	<1	<3	<5	<10	<30	<60	<120	<240	<480	<720	<1080	<1440
Download	0.7%	91.8%	92.5%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Download + Callback	1.5%	93.3%	93.3%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Overall	1.5%	93.3%	93.3%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Figure 6 – Malware Delivered over Email: Detection over Time (Minutes)

Offline Infections

Offline infections are defined as hosts infected with malware outside the corporate network and subsequently attached to the network. Over the course of the test, the Fortinet FortiSandbox-2000E & FortiClient (ATP Agent) detected 93.3% of offline infections. Figure 7 provides a histogram of detection over time. Earlier detection is better.

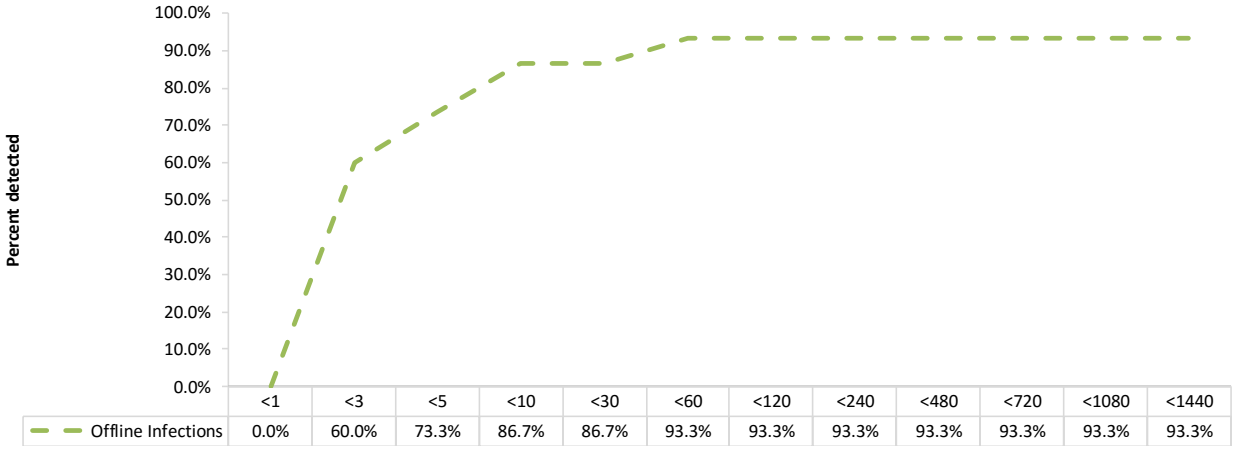


Figure 7 – Offline Infections

Resistance to Evasion Techniques

Evasion techniques are a means of disguising and modifying attacks at the point of delivery in order to avoid detection by security products. If a security device fails to correctly identify a specific type of evasion, an attacker could potentially deliver malware that the device normally would detect. Figure 8 provides the results of the evasion tests for the Fortinet FortiSandbox-2000E & FortiClient (ATP Agent).

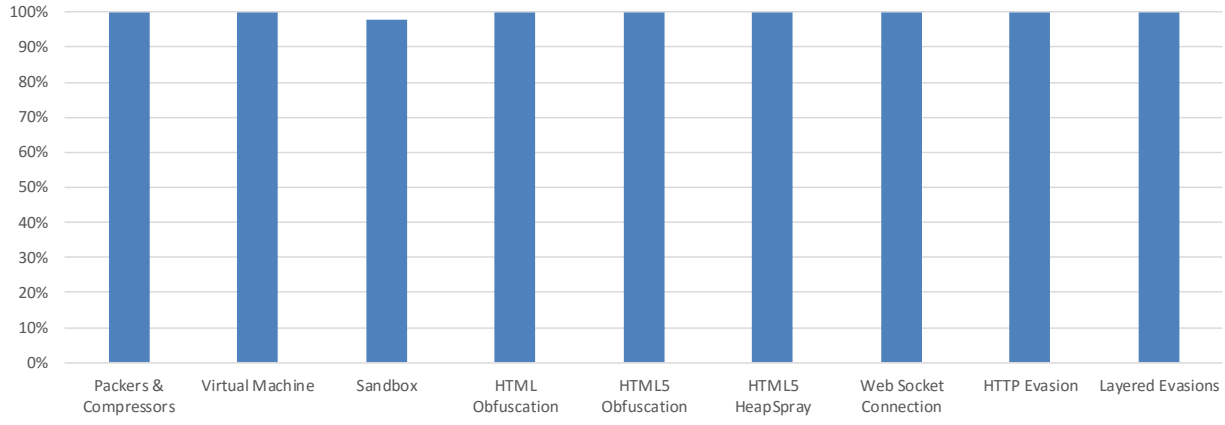


Figure 8 – Resistance to Evasion Results

Network Device Performance

There is frequently a trade-off between security effectiveness and performance; a product's security effectiveness should be evaluated within the context of its performance, and vice versa. This ensures that detection does not adversely impact performance and that no security shortcuts are taken to maintain or improve performance. The NSS performance tests are designed to validate that a network device inspection engine can maintain its detection rate as background traffic increases. All tests in this section are repeated at 25%, 50%, 75%, and 100% of the maximum rated throughput of the system under test (note that the 100% load will actually be less than 100% to allow headroom for malicious traffic). At each stage, multiple instances of malicious traffic are passed and the number detected is logged. The first stage at which one or more attacks is not detected is recorded as the maximum capacity for that test.

HTTP Capacity with No Transaction Delays

These tests stress the HTTP detection engine and determine how the system copes with network loads of varying average packet size and varying connections per second. By creating genuine session-based traffic with varying session lengths, the system is forced to track valid TCP sessions, thus ensuring a higher workload than for simple packet-based background traffic. This provides a test environment that is as close to real-world conditions as can be achieved in a lab environment, while also ensuring absolute accuracy and repeatability.

Each transaction consists of a single HTTP GET request with no transaction delays (that is, the web server responds immediately to all requests). All packets contain valid payload (a mix of binary and ASCII objects) and address data. This test provides an excellent representation of a live network (albeit one biased toward HTTP traffic) at various network loads.

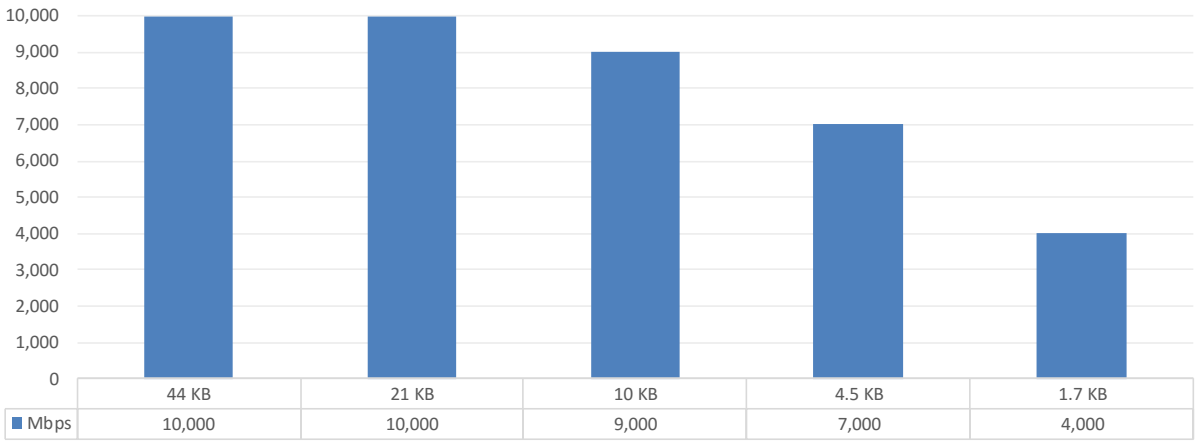


Figure 9 – Detection under Load (HTTP Capacity with No Transaction Delay)

Real-World Traffic Mixes

This test measures the performance of the network device under test in a "real-world" environment by introducing additional protocols and real content while still maintaining a precisely repeatable and consistent background traffic load. The average result is a background traffic load that is closer to what may be found on a heavily utilized "normal" production network. Results are presented in Figure 10.

The Fortinet FortiSandbox-2000Eperformed above the vendor-claimed throughput for all traffic mixes. Fortinet rates this device at 4,000 Mbps.

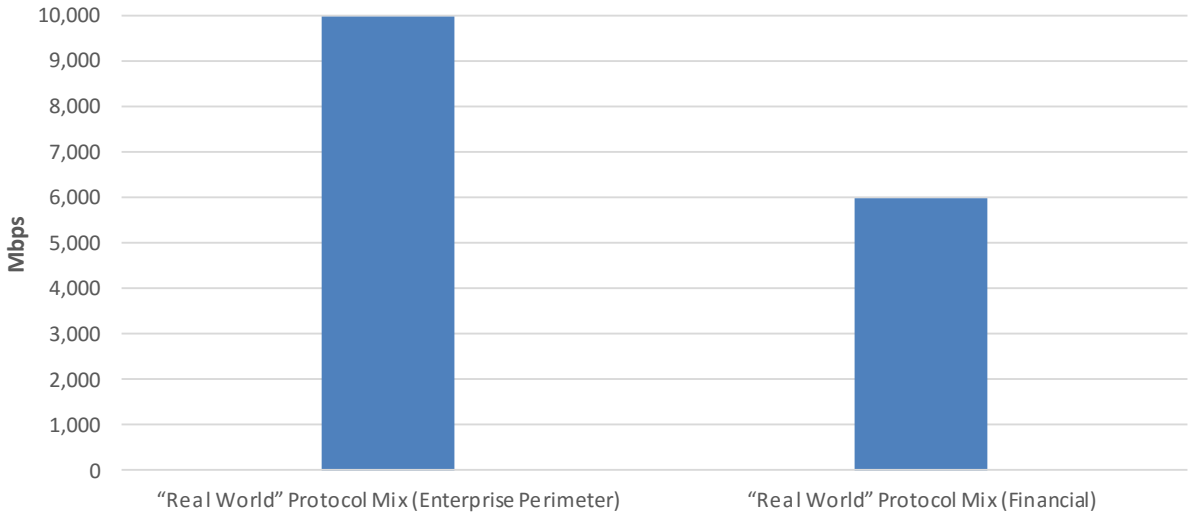


Figure 10 – Detection under Load ("Real-World" Traffic)

Stability and Reliability

Long-term stability is important, since a failure can result in serious breaches remaining undetected and thus not being remediated. These tests verify the stability of the system along with its ability to maintain security effectiveness while under normal load and while detecting malicious traffic. Products that cannot sustain logging of legitimate traffic or that crash while under hostile attack will not pass.

The system is required to remain operational and stable throughout these tests and to detect 100% of previously detected traffic, raising an alert for each. If any malicious traffic passes undetected—caused by either the volume of traffic or by the system failing for any reason—this will result in a fail.

Figure 11 presents the results of the stability and reliability tests for the Fortinet FortiSandbox-2000E.

Stability and Reliability	Result
Detection under extended attack	PASS
Power failure and persistence of data	PASS

Figure 11 – Stability and Reliability Results

Total Cost of Ownership (TCO)

Implementation of security solutions can be complex, with several factors affecting the overall cost of deployment, maintenance, and upkeep. All of the following should be considered over the course of the useful life of the product:

- **Product Purchase** – The cost of acquisition
- **Product Maintenance** – The fees paid to the vendor, including software and hardware support, maintenance, and other updates
- **Installation** – The time required to take the device out of the box, configure it, install it in the network, apply updates and patches, and set up desired logging and reporting
- **Upkeep** – The time required to apply periodic updates and patches from vendors, including hardware, software, and other updates
- **Management** – Day-to-day management tasks, including device configuration, policy updates, policy deployment, alert handling, and so on

For the purposes of this report, capital expenditure (capex) items are included for a single device only (the cost of acquisition and installation).

Calculating the Total Cost of Ownership (TCO)

When procuring a BDS solution for the enterprise, it is essential to factor in both bandwidth and number of users. NSS has found that the malware detection rates of some BDS network devices drop when they operate at maximum capacity. NSS research has shown that, in general, enterprise network administrators architect their networks for up to 2 Mbps of sustained throughput per employee. For example, to support 500 users, an enterprise must deploy 500 agents and/or one network device of 1,000 Mbps capacity.

Users	Mbps per User	Network Device Throughput	Centralized Management
500	2 Mbps	1,000 Mbps	1

Figure 12 – Number of Users

Installation Time

Figure 13 depicts the number of hours of labor required to install each system using only local device management options. The table accurately reflects the amount of time that NSS engineers, with the help of vendor engineers, needed to install and configure the system to the point where it operated successfully in the test harness, passed legitimate traffic, and blocked and detected any prohibited or malicious traffic. This closely mimics a typical enterprise deployment scenario for a single system.

Installation cost is based on the time that an experienced security engineer would require to perform the installation tasks described above. This approach allows NSS to hold constant the talent cost and measure only the difference in time required for installation. Readers should substitute their own costs to obtain accurate TCO figures.

Product	Installation
Fortinet FortiSandbox-2000E v.FSA 2.4.1 & FortiClient (ATP Agent) v.5.6.0.1075	8 hours

Figure 13 – Installation Time (Hours)

Total Cost of Ownership

Calculations are based on 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. Prices are for a 1,000 Mbps single-network BDS and/or 500 software agents and maintenance only; costs for central management solutions (CMS) may be extra.

Product	Purchase	Maintenance /Year	Year 1 Cost	Year 2 Cost	Year 3 Cost	3-Year TCO
Fortinet FortiSandbox-2000E v.FSA 2.4.1 & FortiClient (ATP Agent) v.5.6.0.1075	$52,000	$25,935	$78,535	$25,935	$25,935	$130,405

Figure 14 –3-Year TCO (US$)

- **Year 1 Cost** is calculated by adding installation costs (US$75 per hour fully loaded labor x installation time) + purchase price + first-year maintenance/support fees.
- **Year 2 Cost** consists only of maintenance/support fees.
- **Year 3 Cost** consists only of maintenance/support fees.

For additional TCO analysis, including for the CMS, refer to the TCO Comparative Report.

Appendix: Product Scorecard

Security Effectiveness			
False Positives (Detection Accuracy)	0.06%		
Detection Rate	Download/Drop	Callback + Drop	**Overall**
Exploits			
Drive-by Exploits	95.8%	95.8%	**95.8%**
Social Exploits	66.7%	93.3%	**93.3%**
Malware (various delivery mechanisms)			
HTTP	100.0%	100.0%	**100.0%**
SMTP	100.0%	100.0%	**100.0%**
Off-Line Infections	93.3%		
Evasions	**99.8%**		
Packers & Compressors	100.0%		
Virtual Machine	100.0%		
Sandbox	98.0%		
HTML Obfuscation	100.0%		
HTML5 Obfuscation	100.0%		
HTML5 HeapSpray	100.0%		
Web Socket Connection	100.0%		
HTTP Evasion	100.0%		
Layered Evasions	100.0%		
Performance			
HTTP Capacity with No Transaction Delays	Max Capacity (Mbps)		
44 KB HTTP Response Size – 2,500 Connections per Second	10,000		
21 KB HTTP Response Size – 5,000 Connections per Second	10,000		
10 KB HTTP Response Size – 10,000 Connections per Second	9,000		
4.5 KB HTTP Response Size – 20,000 Connections per Second	7,000		
1.7 KB HTTP Response Size – 40,000 Connections per Second	4,000		
"Real-World" Traffic	Max Capacity (Mbps)		
"Real World" Protocol Mix (Enterprise Perimeter)	10,000		
"Real World" Protocol Mix (Financial)	6,000		
Stability & Reliability			
Detection Under Extended Attack	PASS		
Power Failure and Persistence of Data	PASS		
Total Cost of Ownership			
Ease of Use			
Initial Setup (Hours)	8		
Time Required for Upkeep (Hours per Year)	Contact NSS		
Time Required to Tune (Hours per Year)	Contact NSS		
Expected Costs	US$		
Initial Purchase (hardware as tested)	$52,000		
Installation Labor Cost (@$75/hr)	$600		
Annual Cost of Maintenance & Support (hardware/software)	$25,935		
Annual Cost of Updates (IPS/AV/etc.)	$0		
Initial Purchase (centralized management system)	See Comparative		

Annual Cost of Maintenance & Support (centralized management system)	See Comparative
Total Cost of Ownership	US$
Year 1	$78,535
Year 2	$25,935
Year 3	$25,935
3-Year Total Cost of Ownership	$130,405

Figure 15 – Scorecard

Test Methodology

Breach Detection Systems (BDS) Test Methodology v4.0

A copy of the test methodology is available on the NSS Labs website at www.nsslabs.com.

Contact Information

NSS Labs, Inc.
3711 South MoPac Expressway
Building 1, Suite 400
Austin, TX 78746-8022
USA
info@nsslabs.com
www.nsslabs.com