BREACH PREVENTION SYSTEMS TEST REPORT

Fortinet Advanced Threat Protection (FortiSandbox Cloud with FortiGate 600D v5.6.1, FortiMail Virtual Appliance v5.4.0 and FortiClient ATP Agent v5.6.1.1112)

DECEMBER 13, 2017

Authors – William Dean Freeman (CISSP, CSSLP, GCIH), Jessica Williams

Overview

NSS Labs performed an independent test of the Fortinet Advanced Threat Protection (FortiSandbox Cloud with FortiGate 600D v5.6.1, FortiMail Virtual Appliance v5.4.0 and FortiClient ATP Agent v5.6.1.1112). The product was subjected to thorough testing at the NSS facility in Austin, Texas, based on the Breach Prevention Systems (BPS) Test Methodology v1.1 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 BPS 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					Block Rate	NSS-Tested Throughput	3-Year TCO (US$)
Fortinet Advanced Threat Protection (FortiSandbox Cloud with FortiGate 600D v5.6.1, FortiMail Virtual Appliance v5.4.0 and FortiClient ATP Agent v5.6.1.1112)					99.6%	2,692 Mbps	$20,430
	Drive-by Exploits	Social Exploits	HTTP Malware	Email Malware	Offline Infections	False Positives	Evasions[1]
Block Rate	100.0%	93.3%	99.3%	99.0%	100.0%	0.00%	88.6%
Additionally Detected	0.0%	6.7%	0.5%	1.0%	0.0%	0.00%	NA

Figure 1 –Test Results

Block Rate is defined as the percentage of exploits and malware blocked. The *Additionally Detected* metric depicts the percentage of exploits and malware that is detected but not blocked within 15 minutes.

A BPS with a low block rate will incur less security savings in the event of breach, since additional operational overhead will be required to remediate the effects of a compromised system and protect the business. For detailed TCO analysis, please see the TCO Comparative Report on www.nsslabs.com.

The Fortinet Advanced Threat Protection received a breach prevention block rate of 99.6%. The Fortinet Advanced Threat Protection failed to block 18.2% of Binary Obfuscation Evasions, 100% of Anti-Debugger Evasions, and 33.3% of Anti-Monitoring Evasions tested, which resulted in a weighted evasion score of 88.6%.

The Fortinet Advanced Threat Protection was tested and rated by NSS at 2,692 Mbps, which is lower than the vendor-claimed throughput; Fortinet rates this device at 3,000 Mbps. NSS-Tested Throughput is calculated as an average of the Enterprise Perimeter and Education "real-world" protocol mixes*,* and the 21 KB HTTP response-based tests.

[1] For evasions testing, NSS verifies that the solution is capable of blocking threats, .i.e., it is able to take action against malware and exploits when subjected to various common evasion techniques. Evasions were weighted using a high, medium, or low scale. For additional information, please see the NSS Labs BPS Security Comparative Report, available at www.nsslabs.com.

Table of Contents

Table of Figures

Security Effectiveness

This section aims to verify that the product can block 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 block and report on 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 block known samples and report on them within 15 minutes of initial infection and command-and-control (C&C) callback. Any system that does not block an attack, infection, or C&C callback within the detection window will not receive credit.

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

- **Web-based malware attacks**– The user clicks a link and downloads a malicious application via HTTP.
- **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**– Malware that is embedded in Trojan-horse applications or that leverages exploits in commonly used desktop software.
- **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

It is imperative that a BPS does not suffer from frequent false-positive events, since unlike a breach detection system (BDS) where an event is merely logged, a BPS can take preventative action and block access to malicious software and websites. 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 Advanced Threat Protection demonstrated a false positive rate of 0.00%.

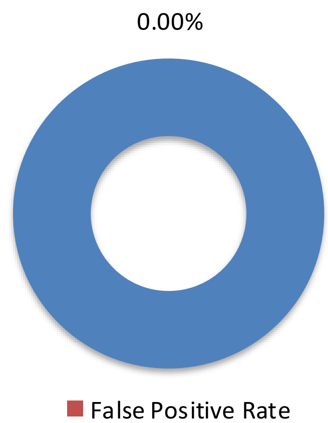


Figure 2 – False Positive Rate

Drive-By Exploits

Figure 3 depicts the results from the drive-by exploit testing. 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 Advanced Threat Protection blocked 100% of drive-by exploits.

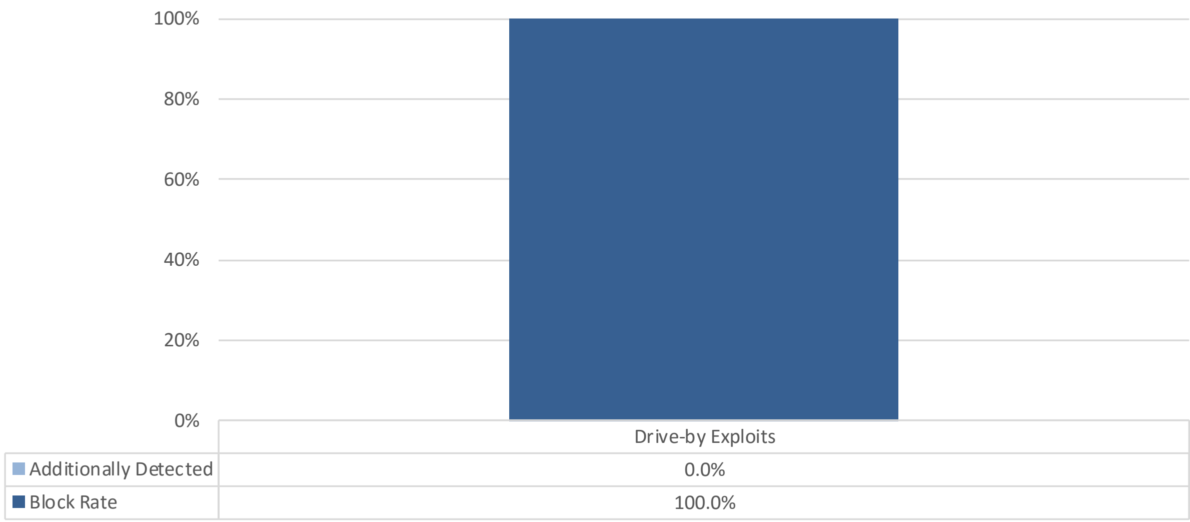
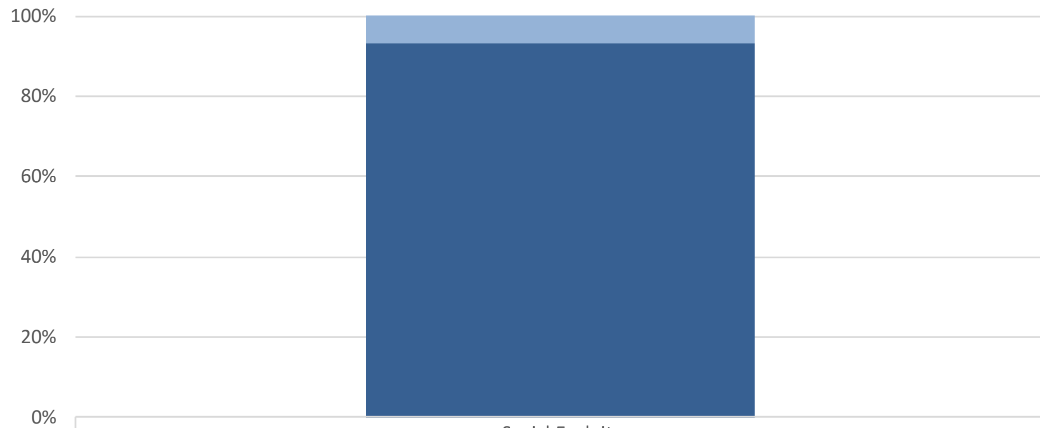


Figure 3 – Malware Delivered by Drive-by Exploits

Social Exploits

Figure 4 depicts the results from the social exploit testing. 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 Advanced Threat Protection blocked 93.3% of social exploits and additionally detected 6.7% of social exploits.

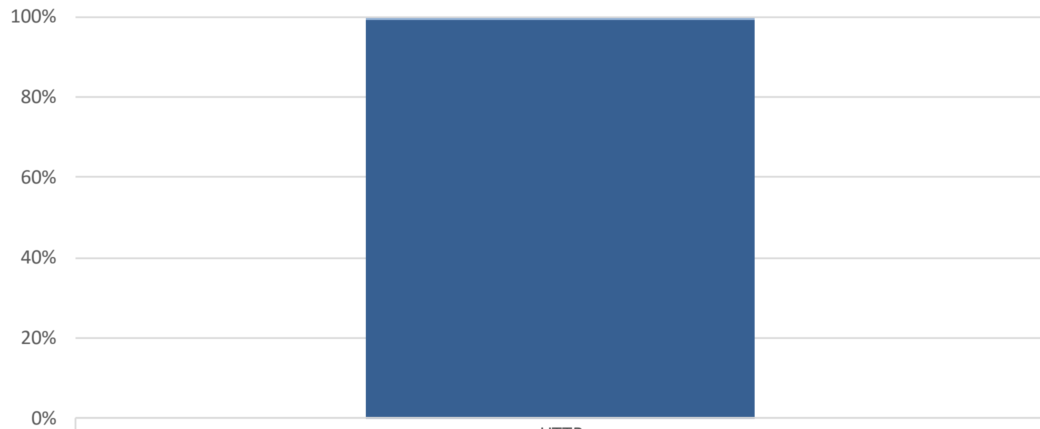


	Social Exploits
Additionally Detected	6.7%
Block Rate	93.3%

Figure 4 – Malware Delivered by Social Exploits

Malware Delivered over HTTP

Figure 5 depicts the results of testing with malware delivered over HTTP. Over the course of the test, the Fortinet Advanced Threat Protection blocked 99.3% of malware delivered over HTTP and additionally detected 0.5% of malware delivered over HTTP.

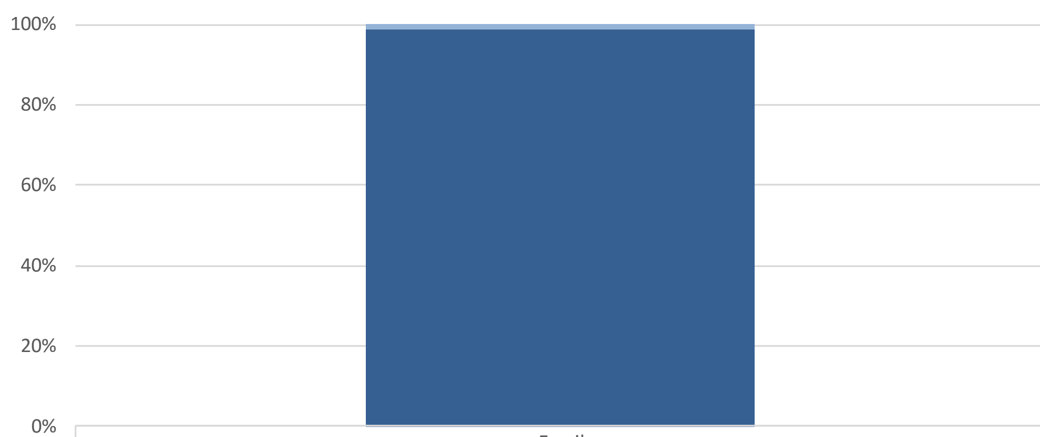


	HTTP
Additionally Detected	0.5%
Block Rate	99.3%

Figure 5 – Malware Delivered over HTTP

Malware Delivered over Email

Figure 6 depicts the results of testing with malware delivered over email. Over the course of the test, the Fortinet Advanced Threat Protection blocked 99.0% of malware delivered over email and additionally detected 1% of malware delivered over email.

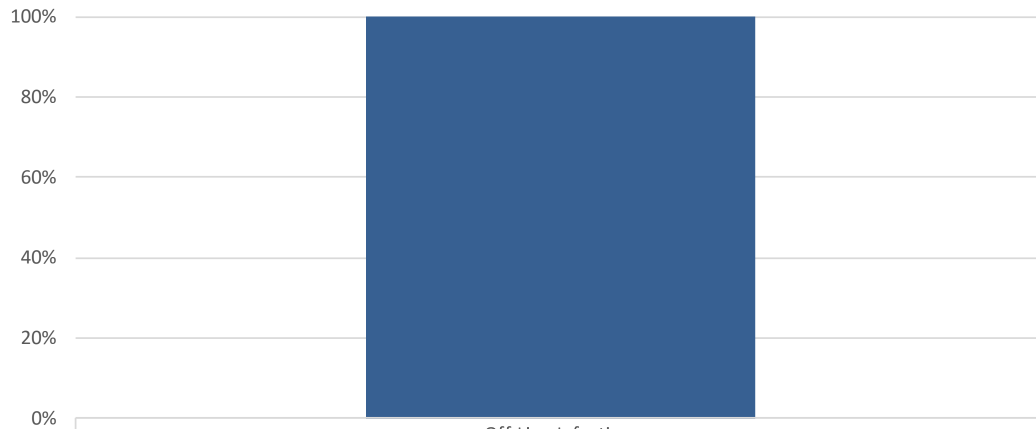


	Email
Additionally Detected	1.0%
Block Rate	99.0%

Figure 6 – Malware Delivered over Email

Offline Infections

In an offline infection, a host (e.g., a laptop) is infected with malware outside a corporate network. Once the host is subsequently attached to the network, the malware should be detected by the security product. Over the course of the test, the Fortinet Advanced Threat Protection blocked 100% of offline infections.

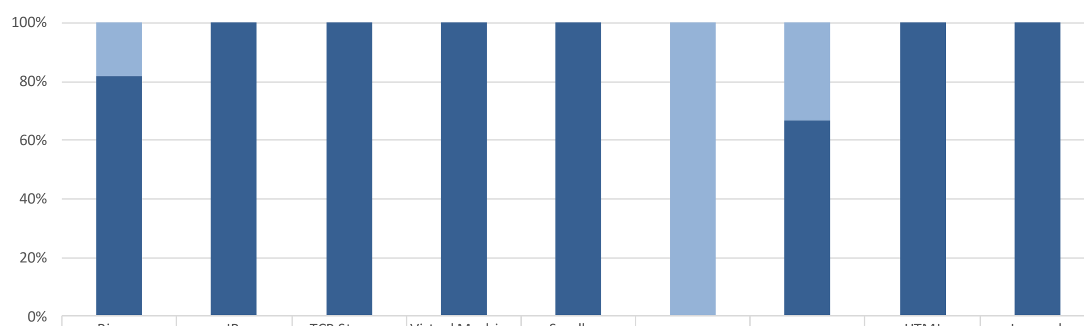


	Off-Line Infections
Additionally Detected	0.0%
Block Rate	100.0%

Figure 7 – Offline Infections

Resistance to Evasion Techniques

Cybercriminals deploy evasion techniques to disguise and modify attacks at the point of delivery in order to avoid detection by BPS products. If a BPS product fails to correctly identify a specific type of evasion, an attacker can potentially deliver malware that the BPS would normally detect. Attackers can modify attacks and malicious code in order to evade detection in a number of ways.



	Binary Obfuscation	IP Fragmentation	TCP Stream Segmentation	Virtual Machine Evasion	Sandbox Evasion	Anti-Debugger	Anti-Monitoring	HTML Obfuscation	Layered Evasions
Additionally Detected	18.2%	0.0%	0.0%	0.0%	0.0%	100.0%	33.3%	0.0%	0.0%
Block Rate	81.8%	100.0%	100.0%	100.0%	100.0%	0.0%	66.7%	100.0%	100.0%

Figure 8 – Resistance to Evasion Techniques

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.

Maximum Capacity

The use of traffic generation appliances allows NSS engineers to create "real-world" traffic at multi-Gigabit speeds as a background load for the tests.

The aim of these tests is to stress the inspection engine and determine how it copes with high volumes of TCP connections per second, application layer transactions per second, and concurrent open connections. All packets contain valid payload and address data, and these tests provide an excellent representation of a live network at various connection/transaction rates.

Note that in all tests the following critical "breaking points"—where the final measurements are taken—are used:

- **Excessive concurrent TCP connections** – Latency within the BPS is causing an unacceptable increase in open connections.
- **Excessive concurrent HTTP connections** – Latency within the BPS is causing excessive delays and increased response time.
- **Unsuccessful HTTP transactions** – Normally, there should be zero unsuccessful transactions. Once these appear, it is an indication that excessive latency within the BPS is causing connections to time out.

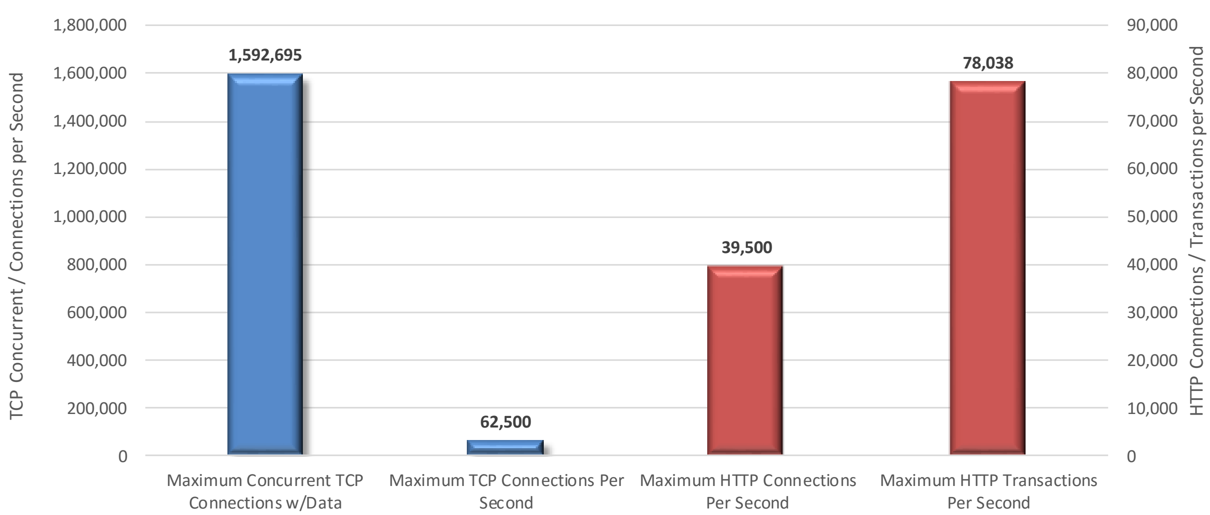
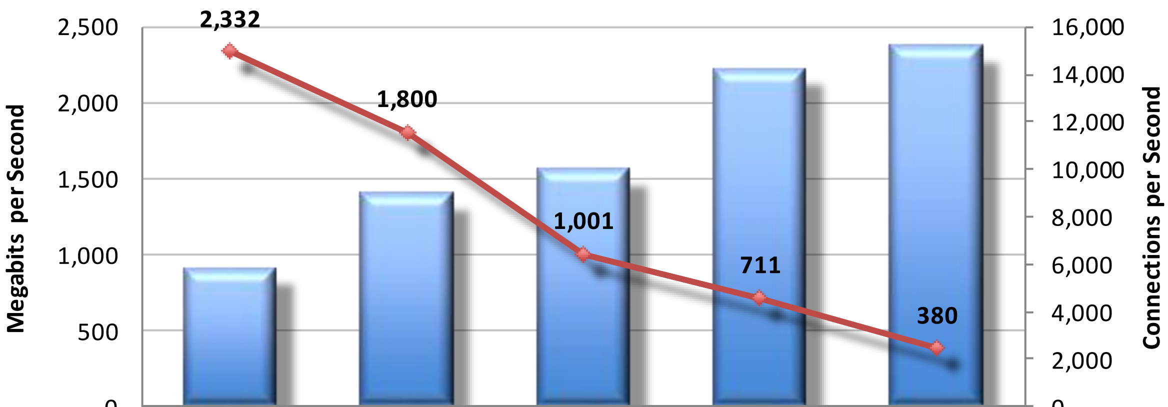


Figure 9 – Concurrency and Connection Rates

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 BPS 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.



	44 KB Response	21 KB Response	10 KB Response	4.5 KB Response	1.7 KB Response
CPS	5,831	9,000	10,010	14,220	15,200
Mbps	2,332	1,800	1,001	711	380

Figure 10 – HTTP Capacity with No Transaction Delays

Application Average Response Time – HTTP

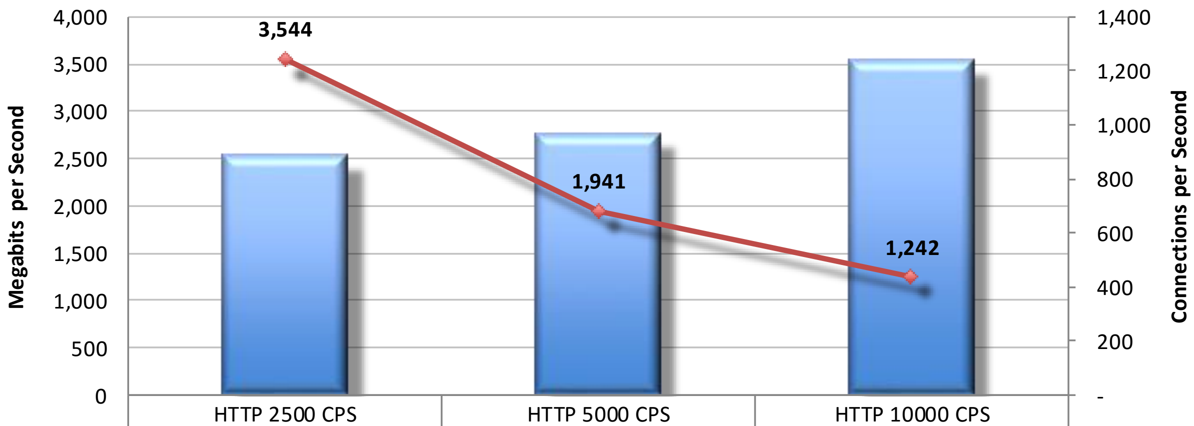
Application Average Response Time – HTTP (at 95% Maximum Load)	Milliseconds
44 KB Response	5.84
21 KB Response	9.19
10 KB Response	3.53
4.5 KB Response	9.97
1.7 KB Response	12.32

Figure 11 – Average Application Response Time (Milliseconds)

HTTP Capacity with HTTP Persistent Connections

These tests determine how the BPS copes with network loads of varying average packet size and varying connections per second while inspecting all traffic. By creating genuine session-based traffic with varying session lengths, the BPS 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 it is possible to achieve in a lab environment, while ensuring absolute accuracy and repeatability.

This test use HTTP persistent connections, with each TCP connection containing 10 HTTP GETs and associated responses. All packets contain valid payload (a mix of binary and ASCII objects) and address data, and the test provides an excellent representation of a live network at various network loads. The stated response size is the total of all HTTP responses within a single TCP session.

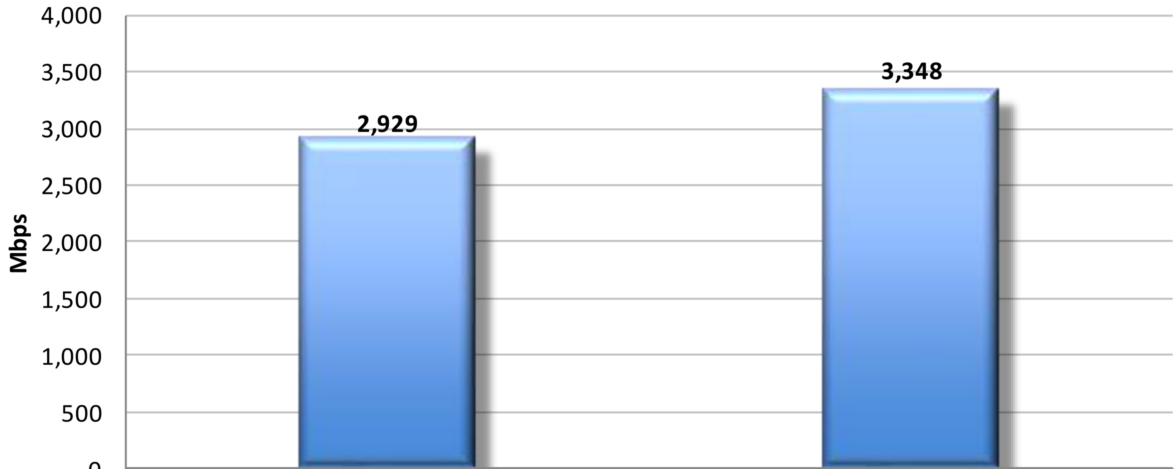


	HTTP 2500 CPS	HTTP 5000 CPS	HTTP 10000 CPS
CPS	886	970	1,242
Mbps	3,544	1,941	1,242

Figure 12 – HTTP Capacity with HTTP Persistent Connections

Real-World Traffic Mixes

This test measures the performance of the system 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 13.



	Real World Protocol Mix (Enterprise Perimeter)	Real World Education
Mbps	2,929	3,348

Figure 13 –Real-World Traffic Mixes

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 TCO analysis, refer to the TCO Comparative Report, which is available at www.nsslabs.com

Calculating the Total Cost of Ownership (TCO)

When procuring a BPS 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 BPS 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 14 – Number of Users

Installation Time

Figure 15 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 Advanced Threat Protection (FortiSandbox Cloud with FortiGate 600D v5.6.1, FortiMail Virtual Appliance v5.4.0 and FortiClient ATP Agent v5.6.1.1112)	8 hours

Figure 15 – 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 BPS 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 Advanced Threat Protection (FortiSandbox Cloud with FortiGate 600D v5.6.1, FortiMail Virtual Appliance v5.4.0 and FortiClient ATP Agent v5.6.1.1112)	$7,349	$4,160	$12,110	$4,160	$4,160	$20,430

Figure 16 –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		
False Positives	0.00%	
	Block Rate	**Additionally Detected**
Exploits		
Drive-by Exploits	100.0%	0.0%
Social Exploits	93.3%	6.7%
Malware (various delivery mechanisms)		
HTTP	99.3%	0.5%
Email	99.0%	1.0%
Offline Infections	100.0%	0.0%
Evasions		
Binary Obfuscation	81.8%	18.2%
IP Fragmentation	100.0%	0.0%
TCP Stream Segmentation	100.0%	0.0%
Virtual Machine Evasion	100.0%	0.0%
Sandbox Evasion	100.0%	0.0%
Anti-Debugger	0.0%	100.0%
Anti-Monitoring	66.7%	33.3%
HTML Obfuscation	100.0%	0.0%
Layered Evasions	100.0%	0.0%
Performance		
Maximum Capacity	**CPS**	
Theoretical Max. Concurrent TCP Connections w/Data	1,592,695	
Maximum TCP Connections Per Second	62,500	
Maximum HTTP Connections Per Second	39,500	
Maximum HTTP Transactions Per Second	78,038	
HTTP Capacity with No Transaction Delays	**CPS**	
2,500 Connections per Second – 44 KB Response	5,831	
5,000 Connections per Second – 21 KB Response	9,000	
10,000 Connections per Second – 10 KB Response	10,010	
20,000 Connections per Second – 4.5 KB Response	14,220	
40,000 Connections per Second – 1.7 KB Response	15,200	
Application Average Response Time – HTTP (at 90% Max Load)	**Milliseconds**	
2,500 Connections per Second – 44 KB Response	5.84	
5,000 Connections per Second – 21 KB Response	9.19	
10,000 Connections per Second – 10 KB Response	3.53	
20,000 Connections per Second – 4.5 KB Response	9.97	
40,000 Connections per Second – 1.7 KB Response	12.32	
HTTP Capacity with HTTP Persistent Connections	**CPS**	
2,500 Connections per Second	886	
5,000 Connections per Second	970	
10,000 Connections per Second	1,242	

Real-World Traffic	**Mbps**
Real-World Protocol Mix (Enterprise Perimeter)	2,929
Real-World Protocol Mix (Education)	3,348
Total Cost of Ownership	
Ease of Use	
Initial Setup (Hours)	8
Time Required for Upkeep (Hours per Year)	See Comparative Report
Time Required to Tune (Hours per Year)	See Comparative Report
Expected Costs	
Initial Purchase (hardware as tested)	$7,349
Installation Labor Cost (@$75/hr)	$600
Annual Cost of Maintenance & Support (hardware/software)	$2,690
Annual Cost of Updates (IPS/AV/etc.)	$1,470
Initial Purchase (enterprise management system)	See Comparative Report
Annual Cost of Maintenance & Support (enterprise management system)	See Comparative Report
Total Cost of Ownership	
Year 1	$12,110
Year 2	$4,160
Year 3	$4,160
3-Year Total Cost of Ownership	$20,430

Figure 17 – Scorecard

Test Methodology

Breach Prevention Systems (BPS) Test Methodology v1.1

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