INDEPENDENT VALIDATION OF FORTINET SOLUTIONS
NSS LABS REAL-WORLD GROUP TESTS

NSS LABS RECOMMENDED

INTRODUCTION

Organizations can get overwhelmed by vendor claims and alleged "silver bullets" when evaluating solutions that can reduce the risk of a data breach. An IT security purchase made solely based on vendor claims is likely to lead to regret. In a recent survey by Forrester Research[i] of next-generation firewall purchase decision makers, 71% surveyed would do more comprehensive testing during the evaluation process if they could do it over again, and 61% would also consider a broader selection of vendors. How do you navigate it all to make good decisions then?

71%
Would do more comprehensive testing during evaluation

61%
Would consider a broader selection of vendors

Fortinet believes that independent, third-party tests provide a critical and impartial measure of the quality of a product, and a mandatory reference for anyone making an IT Security purchase decision. Fortinet is committed to participation in unbiased credible testing so customers can see how we compare to alternative solutions and select the solution that is right for their needs. This commitment is why we consistently submit our products to a large number of third party independent tests for evaluation.

There are many analysts, researchers, and test houses who make it their business to provide their take on the various security solutions available. However, a relatively small number actually evaluate products in real-world, independent conditions. The leader in the independent testing space is NSS Labs.

Fortinet requires the following criteria to be met to participate in a review, test or assessment:

- ✓ Published, clearly defined methodology with customer and vendor input
- ✓ Enterprise customer environment with real-world traffic and current threats
- ✓ Not vendor sponsored or "pay to play"
- ✓ Report and ratings based on quantified criteria and demonstrated performance

WHO IS NSS LABS?

1. World's leading security product testing laboratory
2. Focused exclusively on IT security
3. In-depth security product test reports, research, and analyst services
4. Public methodologies open for vendor review and input
5. Tests conducted regularly and free of charge -- no compensation required for vendor participation
6. CEOs, CIOs, CISOs, and information security professionals rely on NSS to evaluate their security investments

[i] Your Best Defense: Next-Generation Firewalls Enable Zero Trust Security… Best Practices For Evaluating And Implementing A NGFW Forrester Research Inc. July 2015

HOW NSS RATES PRODUCTS: UNDERSTANDING THE NSS LABS SECURITY VALUE MAP

NSS Labs assesses the security effectiveness and performance-adjusted total cost of ownership for each product. They typically publish their findings in a number of different reports starting, at the highest level with a summary of results called a "Security Value Map" or SVM. The SVM illustrates the relative value of security investment options by mapping security effectiveness and relative value of tested products. Each technology area – NGFW, IPS, WAF, Sandbox etc. – has its own SVM.
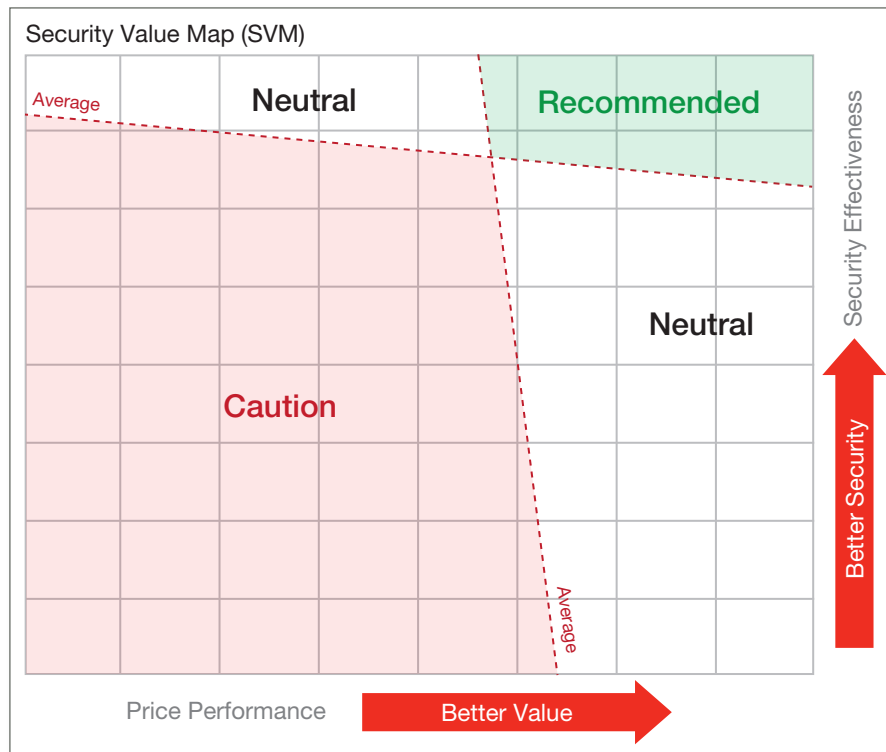
X-AXIS:

3 year TCO per protected unit of measure (Megabit per second, Connection per second)

Y-AXIS:

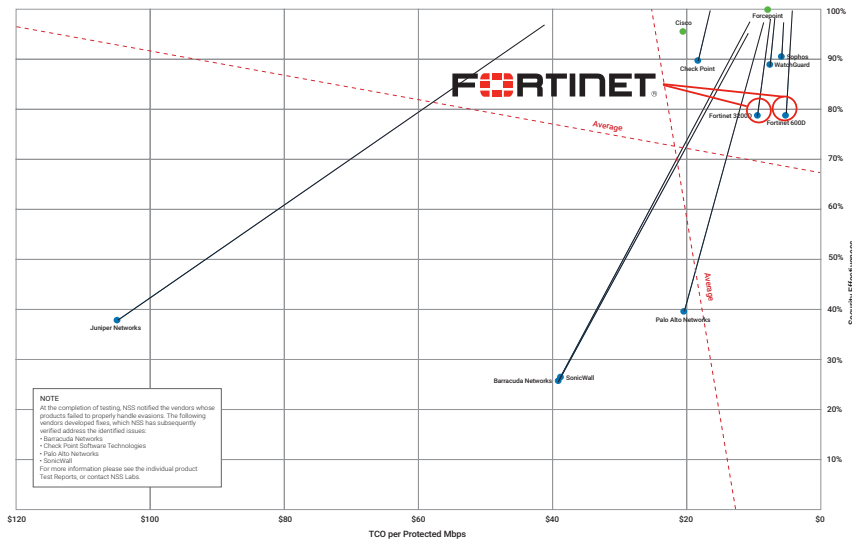Security Effectiveness (block rate)

4 QUADRANTS:

Upper-right: "Recommended", products that provide an above average level of security effectiveness and value for money

Lower left: "Caution", products that offer below average value and security effectiveness

Upper left/Lower Right: "Neutral", may still be worthy of consideration depending on budget limitations.

The following is a review the most current SVMs across several key IT security technologies and offerings. SVMs pictured are the most current version as of date of publication of this document.

NEXT GENERATION FIREWALL (NGFW)
SECURITY VALUE MAP™

NOTE
At the completion of testing, NSS notified the vendors whose products failed to properly handle evasions. The following vendors developed fixes, which NSS has subsequently verified address the identified issues:
• Barracuda Networks
• Check Point Software Technologies
• Palo Alto Networks
• SonicWall
For more information please see the individual product Test Reports, or contact NSS Labs.

NEXT-GENERATION FIREWALL TEST (2017)
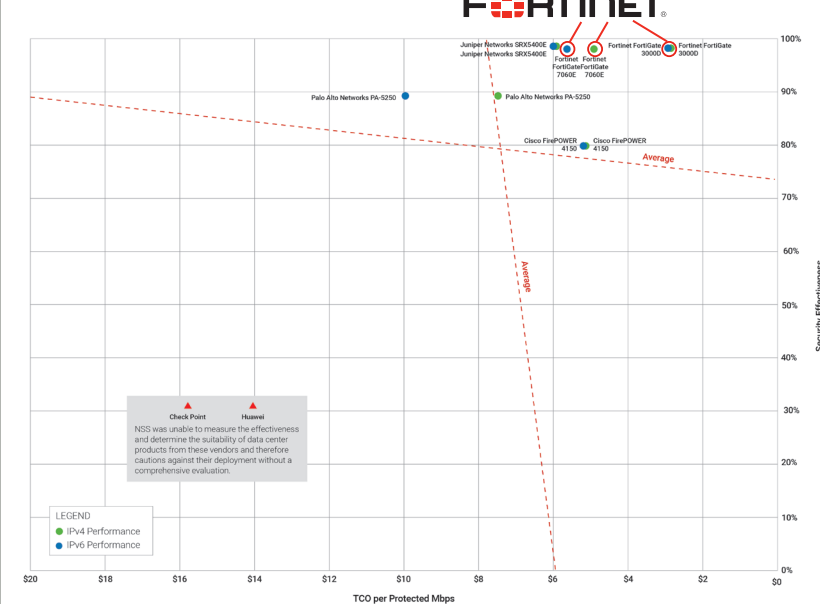
FortiGate 600D and 3200D

Capabilities Tested:

- Firewall
- Intrusion Prevention
- Application Control
- Evasions

Results:

✓ "Recommended" for both models

✓ 99.47% security effectiveness

✓ Highest overall performance (tested at over 18Gbps) with lowest latency

✓ Highest HTTPS performance and least degradation

✓ Best TCO per protected Mbps

DATA CENTER SECURITY GATEWAY (DCSG)
SECURITY VALUE MAP™

NSS was unable to measure the effectiveness and determine the suitability of data center products from these vendors and therefore cautions against their deployment without a comprehensive evaluation.

LEGEND
● IPv4 Performance
● IPv6 Performance

DATA CENTER SECURITY GATEWAY TEST (2017)

FortiGate 7060E and 3000D
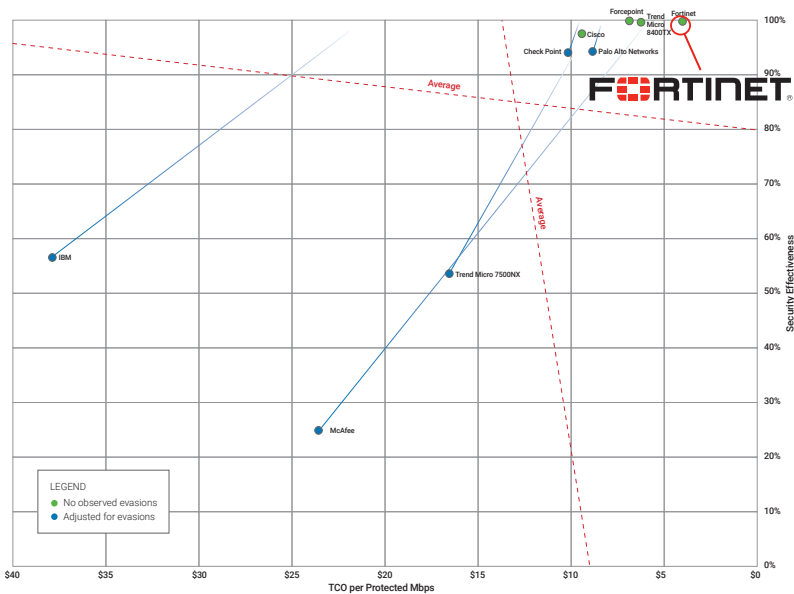
Capabilities Tested:

- Data Center Firewall
- Data Center Intrusion Prevention
- IPv4 and IPv6 Performance
- Evasions

Results:

✓ "Recommended" for both models

✓ 97.87% and 97.97% security effectiveness

✓ 100% evasions blocked

✓ Highest overall performance with lowest latency

✓ Fastest IPS performance (over 130Gbps for FG-7060E)

✓ Equally impressive IPv4 and IPv6 performance

✓ Best TCO per protected Mbps

NEXT-GENERATION INTRUSION PREVENTION (NGIPS)
SECURITY VALUE MAP™

LEGEND
● No observed evasions
● Adjusted for evasions

Security Effectiveness

TCO per Protected Mbps

NEXT-GENERATION INTRUSION PREVENTION TEST (2017)

**FortiGate 600D**

Capabilities Tested:

- Intrusion Prevention Systems (IPS)
- Application Control
- CAWS – Live exploits
- Client and Server focus

Results:

- ✓ "Recommended"
- ✓ 99.71% overall security effectiveness
- ✓ 100% evasion avoidance
- ✓ 100% live zero-day detection (CAWS)
- ✓ Best value (under $4 per protected Mbps)

FORTINET
Fortinet FortiGate 600D v5.x.x
NEXT GENERATION
INTRUSION PREVENTION SYSTEM
NSS
RECOMMENDED

WEB APPLICATION FIREWALL (WAF)
SECURITY VALUE MAP™

Security Effectiveness

TCO per Protected CPS
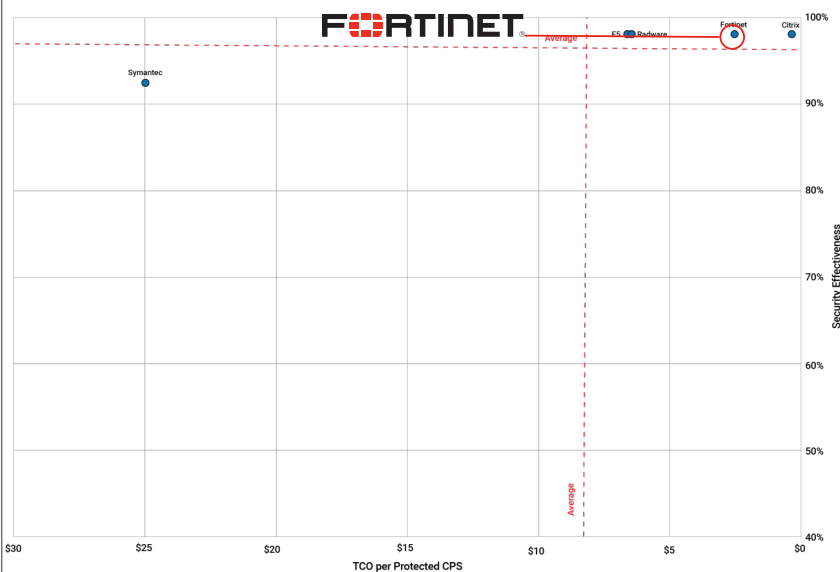
WEB APPLICATION FIREWALL TEST (2017)
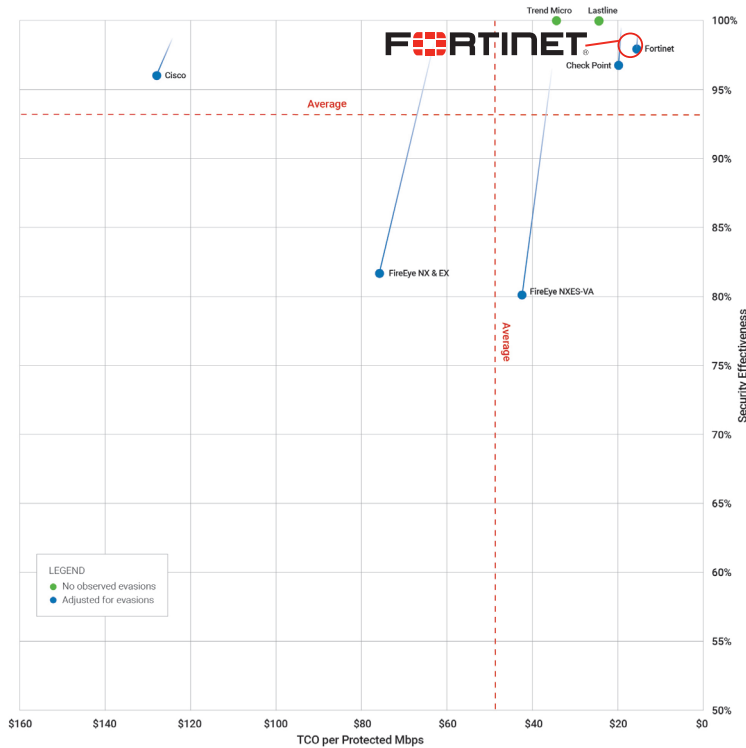
FortiWeb 3000E

Tested against:

- Cookie Manipulation
- URL Manipulation
- SQL Injection
- Cross-site Scripting
- Evasion Tests

Results:

- ✓ "Recommended"
- ✓ 98.1% block rate
- ✓ Perfect scores in 9 of 10 OWASP categories

NSS
RECOMMENDED

BREACH DETECTION SYSTEMS (BDS)
SECURITY VALUE MAP™

BREACH DETECTION SYSTEMS TEST (2017)

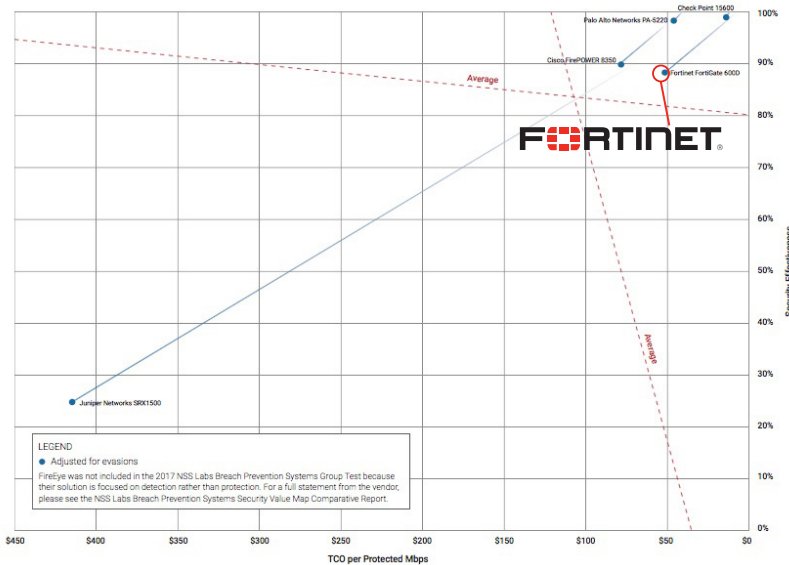**FortiSandbox 2000E with FortiClient**

Capabilities Tested:

- HTTP, SMTP, Offline Malware
- Drive-by & Social Exploits, Doc-jacking, Evasions…
- Time-to-detect, Throughput, Value/TCO

Results:

- ✓ "Recommended"
- ✓ 99% overall detection, 100% web/email
- ✓ Less than 0.1% false positive rate
- ✓ Lowest TCO
- ✓ Rated 8.6 Gbps throughput, 2X claimed rate

BREACH PREVENTION SYSTEMS (BPS)
SECURITY VALUE MAP™

BREACH PREVENTION SYSTEMS TEST (2017)

FortiSandbox, FortiGate, FortiMail and FortiClient

Capabilities Tested:

- Exploits, malware, evasions
- Across web, email and endpoint
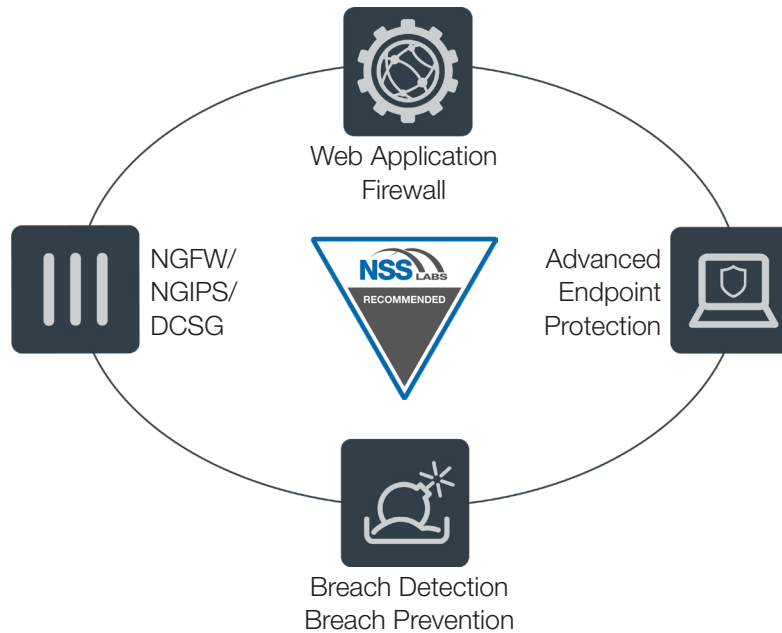- Throughput, TCO, false positives

Results:

- ✓ "Recommended"
- ✓ 99.6% block rate
- ✓ 0% false positives

PUTTING IT ALL TOGETHER – THE ONLY EDGE TO ENDPOINT SOLUTION "RECOMMENDED" BY NSS LABS

By participating in these tests, enterprises and Fortinet, have an indepedent measure of how our products rate against real-world enterprise requirements as well as alternative offerings. Earning "Recommended" ratings in each of the preceding NSS Labs tests, Fortinet stands out as the only vendor to provide an Advanced Threat Protection Solution that is NSS Labs "Recommended" from the edge to the endpoint.

Web Application Firewall

NGFW/ NGIPS/ DCSG

NSS LABS RECOMMENDED

Advanced Endpoint Protection

Breach Detection Breach Prevention

Looking at the 7-year summary of Fortinet ratings in NSS Labs group tests, a pattern emerges of consistent improvement and excellence, a growing list of "Recommended" ratings, and our ongoing commitment to participation in all relevant NSS Labs tests.

Product	2011	2012	2013	2014	2015	2016	2017
Firewall	Neutral		Recommended				Tested*
NGFW		Neutral	Recommended	Recommended		Recommended	Recommended
Data Center Security Gateway							Recommended
Data Center IPS				Neutral		Recommended	
NGIPS					Recommended	Retested & Passed	Recommended
Breach Detection				Recommended	Recommended	Recommended	Recommended
Breach Prevention							Recommended
Web Application Firewall				Recommended			Recommended
Adv. Endpoint Protection					Recommended		Recommended
DDoS						Neutral	

NSS Labs Data Center Firewall test, April 2017. No SVM/recommendations published.

As of January 2018

"Real-world third-party validation is an essential resource for enterprises considering security products to help cut through confusion caused by vendor marketing, NSS Labs' testing continues to demonstrate Fortinet's commitment to meet high industry standards for security detection, performance, reliability, management and value."

- Fortinet CEO Ken Xie

FORTINET'S UNPARALLELED COMMITMENT TO INDEPENDENT TESTING

Earning a Recommended rating from NSS Labs indicates that a product has performed well and deserves strong consideration. Only the most effective and best value products earn a Recommended rating from NSS—regardless of vendor market share, size or brand recognition. In a broad set of the most recent NSS Labs reports, Fortinet has consistently earned "Recommended" ratings. In NSS Labs' CAWS real-time service, customers can also see how Fortinet consistently delivers highly effective security over time.

Fortinet's commitment to independent testing and certification even extends beyond NSS Labs. ICSA, AV Comparatives, Virus Bulletin and other independent testing organizations have also consistently validated the effectiveness of Fortinet solutions. At the 2015 ICSA Labs awards reception, Fortinet was honored with ICSA's prestigious Excellence in Information Security Testing (EIST) award. Fortinet was recognized for outstanding achievement in information security certification testing for 10 years running.

RECOMMENDATION AND CONCLUSION

To avoid the regret expressed by a majority of IT security purchasers in the Forrester study, avoid biased sources of information during your next IT security purchase evaluation.

- ✓ Consult independent, objective sources like NSS Labs to separate the truth from the hype.
- ✓ Conduct a bake off – either in-house or outsourced to a testing specialist. Test with real-world traffic loads to ensure the products can meet your requirements with the appropriate features activated.
- ✓ Select based on your criteria– effectiveness, ease of use, performance, price, vendor history and more may have a role to play.

Since its inception, Fortinet has committed to consistently proving the efficacy of its solutions through stringent independent testing and certification. The company has received more certifications to validate its solutions than any other network security vendor. These test results are proof that — in real world traffic and deployment scenarios — our products will beat the competition and perform as advertised.

www.fortinet.com

January, 2018