

REPORT

Test Results on the Fortinet FortiWiFi 60E vs. Meraki MX Using Ixia's BreakingPoint Network Security Strike Pack

July 2019



Background

It seems nearly all network security vendors make claims about their solutions being the most effective and/or having the lowest TCO. When evaluating security products, how can a buyer know which claims are true? Independent testing from third parties such as NSS Labs and ICSA Labs is one way. In-house testing with an independent testing product is another. When combined, the results offer even more insight into whether product claims are accurate or not.

Fortinet’s technical marketing team used the BreakingPoint Strike Pack independent testing product to determine the security effectiveness of the Meraki MX65W and compared the results to the same tests performed on the FortiWiFi 60E.

Testing Methodology

The BreakingPoint test creates a real-world environment with a complete range of threats and applications. All BreakingPoint tests were performed with customer specification (predefined) and recommended settings.

- The goal was to test security effectiveness.
- Strike Level 3 was used, which includes all high-risk vulnerabilities, worms, and backdoors. This list contains approximately 480 strikes and usually completes in less than three minutes.
- The vendors’ configuration best practices were followed.
- The same tests were run on the FortiGate 61E and the Meraki MX65W.

Vendors	Version	Strike Pack
FortiWiFi 60E	6.2	Strike Level 3
Cisco Meraki MX65W	14.39	Strike Level 3
BreakingPoint	8.50.22.25	

Table 1: Product details.

Fortinet Deployment

- FortiWiFi 60E was tested in route mode.
- Tests were done from LAN to WAN (client side).
- Security services were enabled.

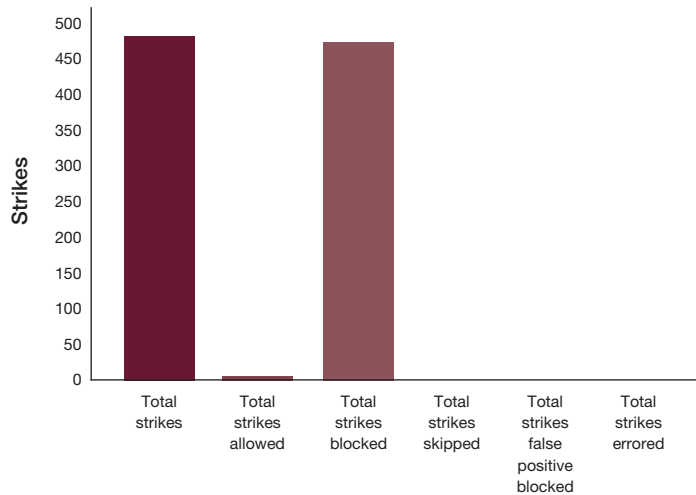


Figure 1: Profile of FortiWiFi 60E with the max security enabled.

Fortinet FortiWiFi 60E Test Results

- Block rate: 99.38%
- Allow rate: 0.619%

Measurement	Value (Strikes)
Total strikes	480
Total strikes allowed	3 0.625%
Total strikes blocked	477 99.375%
Total strikes skipped	0
Total strikes false positive blocked	0
Total strikes errored	0

Table 2: Details of Fortinet Strike Test.

Meraki MX65W Deployment

- Meraki MX was tested in route mode.
- Meraki was tested from a single direction, from LAN to WAN (client side).

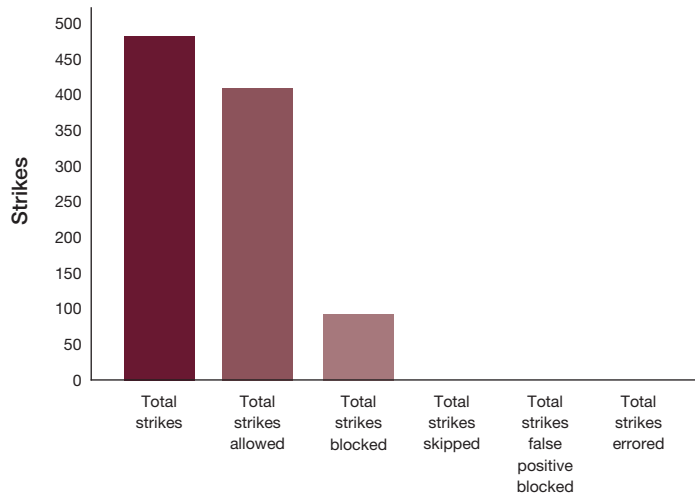


Figure 2: Meraki MX65W deployment.

Meraki Test Results

- Block rate: 15.4%
- Allow rate: 84.5%

Measurement	Value (Strikes)
Total strikes	480
Total strikes allowed	406 84.583%
Total strikes blocked	74 15.417%
Total strikes skipped	0
Total strikes false positive blocked	0
Total strikes errored	0

Table 3: Details of Meraki Strike Test.

Total Cost of Ownership (TCO)

Product	Strike Pack Result	Three-Year TCO	Third-Party Validations (NSS Labs, ICSA)
Fortinet FortiWiFi 60E	99.3% block rate	\$2,250 Includes: 360 protection (FortiCare plus application control, IPS, antivirus, web filtering, antispam, FSA cloud, Security Rating Service, Secure SD-WAN, cloud assisted monitoring, SD-WAN overlay control VPN, FortiManager/ FortiAnalyzer Cloud, industrial security, Forti-Converter, and FortiCASB (up to five users))	NSS Labs, ICSA
Meraki MX65W (Meraki offers an annual and multiyear subscription.)	15% block rate	\$2,845 Includes: advanced security license and 24x7 class support	None

Table 4: Fortinet total cost of ownership.

Fortinet Demonstrated Superior Effectiveness

Meraki’s solution fails to block a high number of exploits and DoS attacks in comparison to Fortinet. Meraki claims MX65W is simple to deploy, but the security factor is of concern. MX65W has a limited IPS/IDS which uses a subset signature from Sourcefire/Snort/Firepower.

Further, Meraki’s WAN link limitations could potentially compromise the whole network should the cloud lose connectivity from the internet.

Fortinet came out on top with a better security effectiveness rating, lower TCO, and validations from NSS Labs and ICSA. The combination of these factors provides customers with the peace of mind that they are deploying a best-in-class solution to secure their organizations.



www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

July 27, 2019 11:19 AM