

## **Cisco Systems, Fortinet, Palo Alto Networks and SonicWall are First Four Security Vendors to Achieve NetSecOPEN-Certified Performance Results**

*Certification Enables True Understanding of Real-World Performance of Fully Configured Security Solutions for Apples-to-Apples Evaluation and Realistic Planning*

**Harrisburg, PA – February 19, 2020** – NetSecOPEN, the first industry organization focused on the creation of open, transparent network security performance testing standards, today announced that Cisco, Fortinet, Palo Alto Networks and SonicWall are the first four security vendors to achieve certified performance results through open, standardized testing developed by NetSecOPEN and adopted by the Internet Engineering Task Force (IETF). These achievements represent a critical milestone on the path to accurate and reliable evaluation of the real-world performance of fully configured, realistically deployed security solutions. They validate NetSecOPEN’s vision of closing the gap between proprietary performance metrics and the actual observed performance of security solutions. Performance that is certified as meeting the NetSecOPEN standard enables “apples-to-apples” evaluation and realistic planning for potential customers.

Today, certification of security product performance is typically conducted by independent testing laboratories that use proprietary testing methodologies. Since the methodologies and test criteria differ from lab to lab, apples-to-apples evaluations of security products pose a challenge for enterprise buyers. NetSecOPEN was formed to bring greater transparency, consensus, and standardization to testing and to integrate real-world factors into the methodology.

“As the creators and authors of Snort and a founding member of NetSecOPEN, we firmly believe in the power of community and open standards to improve security outcomes,” said Jeff Reed, SVP of Product, Security Business Group, Cisco. “Cisco is committed to being our customers’ most trusted security partner, and we look forward to continuing our work with NetSecOPEN to advance and improve open testing standards in our industry.”

“Fortinet is committed to delivering the best threat protection performance and low latency that enterprises require via our purpose-built security processor (SPU) technology. We are pleased to report the certified performance of Fortinet’s FortiGate 500E Next-generation Firewall, tested under real-world conditions,” said John Maddison, EVP of Products and CMO at Fortinet. “As a Founding Member of NetSecOPEN, we believe third-party validation, such as NetSecOPEN-certified metrics, is important to help customers make informed decisions and choose the best possible solution for their organization.”

“As a Founding Member of NetSecOPEN, Palo Alto Networks is committed to transparent, real world testing to help buyers evaluate how security products will perform in their actual environments,” said AJ Shipley, vice president of product management, security services at Palo Alto Networks. “Achieving NetSecOPEN-certified performance further validates our prevention-first philosophy with our industry-leading PA-3250 Next-Generation Firewalls, which help keep our customers a step ahead of adversaries with an architecture that is easy to deploy and operate.”

“Because SonicWall is committed to delivering best-in-class cybersecurity without compromising network performance, we believe that delivering NetSecOPEN-certified metrics is invaluable in helping organizations and technology partners of all sizes make informed decisions,” said Atul Dhablania, Senior Vice President and Chief Operating Officer, SonicWall. “As a founding member of NetSecOPEN, we are pleased to report the certified performance of the SonicWall NSA 4650 firewall. This apples-to-apples comparison provides security buyers with validation of real-world performance and security effectiveness of next-generation firewalls when fully configured for realistic conditions.”

The first two labs certified by NetSecOPEN, the University of New Hampshire InterOperability Laboratory (UNH-IOL) and The European Advanced Networking Test Center (EANTC AG), conducted the standardized testing.

“These first certifications establish a vital milestone on the road to performance results based on open, transparent testing standards for network security equipment that eliminate disruptive surprises and support equal, informed comparison of solutions,” said Brian Monkman, executive director of NetSecOPEN. “The days of opaque, meaningless testing results with no connection to real-world usage are numbered. We are proud to experience such momentum and progress, bringing us closer to making open network security testing standards a universal reality.”

Formed in 2017, NetSecOPEN members collaborate through working groups to help create testing standards and guidance that achieve consistent, open, repeatable evaluations and stated results. Founding Members include top security vendors: Check Point Software, Cisco Systems, Fortinet, Palo Alto Networks, SonicWall, Sophos, and WatchGuard. Founding Members also include testing equipment vendors IXIA and Spirent and testing labs EANTC and UNH-IOL.

For further information and assistance, e-mail [info@netsecopen.org](mailto:info@netsecopen.org). The NetSecOPEN certifications can be found at <http://www.netsecopen.org/certifications>.

## **About NetSecOPEN**

NetSecOPEN is a network security industry group in which network security vendors, tool vendors, labs, and enterprises collaborate to create open and transparent testing standards. The goal of the group is to create a suite of standards that can be used for the evaluation and/or certification of network security products. The NetSecOPEN standards will provide guidelines and best practices for testing modern network security infrastructure.

NetSecOPEN is working toward being certified as a standards body that will oversee the creation and updating of standards. Additionally, NetSecOPEN will oversee evaluation testing by network security product vendors and certification testing conducted by labs against the standards. Anyone with a vested interest in the outcome can participate in the creation or updating of the standards. These efforts will be conducted in an open and transparent manner, with drafts of the standard, project updates future plans posted at <https://www.netsecopen.org>.

# # #

**Contact**      Michelle Schafer  
                     Merritt Group

Direct Tel      +1-703-390-1525  
                     +1-703-403-6377 (mobile)

E-mail          [schafer@merritgrp.com](mailto:schafer@merritgrp.com)