



## Frequently Asked Questions

### 1 What is NetSecOPEN?

NetSecOPEN is a non-profit, membership-driven organization developing open standards for testing of network security products. Formed in 2017, the organization is supported by a number of the world's leading security product vendors, test equipment vendors and testing laboratories.

### 2 Who are the members?

NetSecOPEN founding members are some of the world's leading security product vendors, test equipment vendors and testing laboratories. Security product vendors include Cisco, Fortinet, Palo Alto Networks, SonicWall, Sophos and WatchGuard. Test equipment vendors IXIA, Spirent and Viavi are members, as are test labs EANTC and UNH-IOL. NetSecOPEN is currently in discussions with a number of other prospective members.

A list of the current NetSecOPEN members can be found at <https://www.netsecopen.org/>.

### 3 Why was NetSecOPEN formed?

Certification of security product performance today is typically conducted by independent testing laboratories using proprietary testing methodologies. Since the methodologies and test criteria differ from lab to lab, "apples-to-apples" evaluations of security products are challenging for the enterprise buyers. NetSecOPEN believes that greater transparency, consensus and standardization around testing methodology are needed, and that real-world factors need to be integrated into the testing methodology.

### 4 Why performance testing?

There are no recent up to date relevant open test standards for network security performance testing. In the last 10 years networks have transitioned from 80% unencrypted HTTP to the opposite today with, in many enterprises, over 80% of the perimeter traffic encrypted with HTTPS and modern secure cipher suites.

This has led to many proprietary methods to determine performance of security solutions. NetSecOPEN addresses this with standards to close the often-wide gap in performance between proprietary performance metrics and observed real-world performance of security solutions.



**5 What is the difference between NetSecOPEN and other open performance testing specifications groups such as the IETF benchmark working group?**

NetSecOPEN builds on the work from other groups such as the IETF Benchmark Working Group. Where, for example, the IETF defines how to measure bandwidth of a Firewall, NetSecOPEN applies this to a world with predominantly encrypted HTTPS and how modern security solutions identify applications and look for security threats.

**6 Was NetSecOPEN formed specifically as an alternative to commercial testing labs, such as NSS?**

Not at all, in fact two of the industry's testing labs are founding members: EANTC and UNH-IOL. NetSecOPEN was founded because of a real need to have transparent, open tests of the performance impact of Next Generation Firewall solutions in real world conditions that could be fully compared with other solutions. In other words, it's essential to have apples-to-apples performance tests that realistically portray the impact a NGFW has on networks. The organization exists to fulfill a need and to establish a new way of creating tests that are open, transparent and collaboratively created. NetSecOPEN is not meant as an alternative organization.

**7 Why are companies working with their competitors in NetSecOPEN?**

While many of these vendors and labs compete with one another in the marketplace, they recognize that a common, standards-based open testing methodology, based on real-world criteria, will build confidence among buyers of security products, thus creating greater opportunities for all participants in the global security market.

**8 What is special about the NetSecOPEN testing standard?**

It was developed jointly by the members. It includes a real-world traffic mix, which includes 400 encryption certificates and 10,000 unique URLs. This real-world aspect of the testing methodology is unique to NetSecOPEN and provides a more accurate picture of the load performance that security products face.

**9 Isn't NetSecOPEN a way to lock out certain labs by creating a testing methodology that's stacked in the members' favor?**

Just the opposite. NetSecOPEN is member-driven and open to all interested vendors and testing organizations. The NetSecOPEN testing standard is recognized by the IETF, and available to anyone at <https://datatracker.ietf.org/wg/bmwg/documents/>. NetSecOPEN methodology was developed in consultation with the current membership and will continue to evolve as new members join, and as a new generation of security products comes to market.

**10 Why would NGFW vendors become members and participate in NetSecOPEN if the results from the organization's tests might possibly present unflattering comparisons and show their products in an unfavorable light?**

It is in everybody's best interest to have the means of knowing exactly what kind of effect on performance an NGFW will have on real networks under real operating conditions. The MPG test for automotive fuel efficiency enabled buyers to know what mileage a given car can provide per gallon of gas. The key to this metric is a transparent, repeatable testing procedure that allows apple-to-apple comparisons of cars. Having this doesn't specifically hurt a car manufacturer. There are other important factors to consider, such as price, acceleration, safety, comfort, etc.

**11 What will prevent NetSecOPEN from being the victim of its own open, collaborative approach so that member squabbling prevents a test standard from being finalized?**

The standards we are driving are more matters of specification and clarity or the "how" rather than the "what." We want to see testing that is repeatable anywhere and enables true apples-to-apples comparisons.

**12 Where can I find NetSecOPEN certification reports?**

The certification and testing lab reports can be found at - <https://www.netsecopen.org/certifications>.

**13 Will NetSecOPEN stay focused on performance evaluations and impact on networks, or will the organization later drive testing standards for security?**

NetSecOPEN is a membership-driven organization, so the focus will depend on the direction set collectively by the members. Since many existing security tests in the industry have not been updated in years and do not reflect current conditions and challenges, it is likely that NetSecOPEN will take on standards for security testing in the future if members direct us in that way.

**14 Will NetSecOPEN broaden its scope to tests involving other types of security solutions?**

Yes. NGFWs are a starting point, and one with a great deal of urgency to address, since too many organizations have been surprised and hampered by not knowing what effect a NGFW will have on a network. NetSecOPEN was determined to start with focus and solve one issue extremely well before going on to a next.