DARKReading

NetSecOPEN

MAY 2022

# What Every Enterprise Should Know About Security Product Testing

Test, but verify: With open-testing organizations offering security product testing, companies now have more nonbiased options for evaluating security products for purchase. But you should also take into account your existing security posture.

Brought to you by informa tech

Sponsored by

University of New Hampshire InterOperability Laboratory

INSIDE:



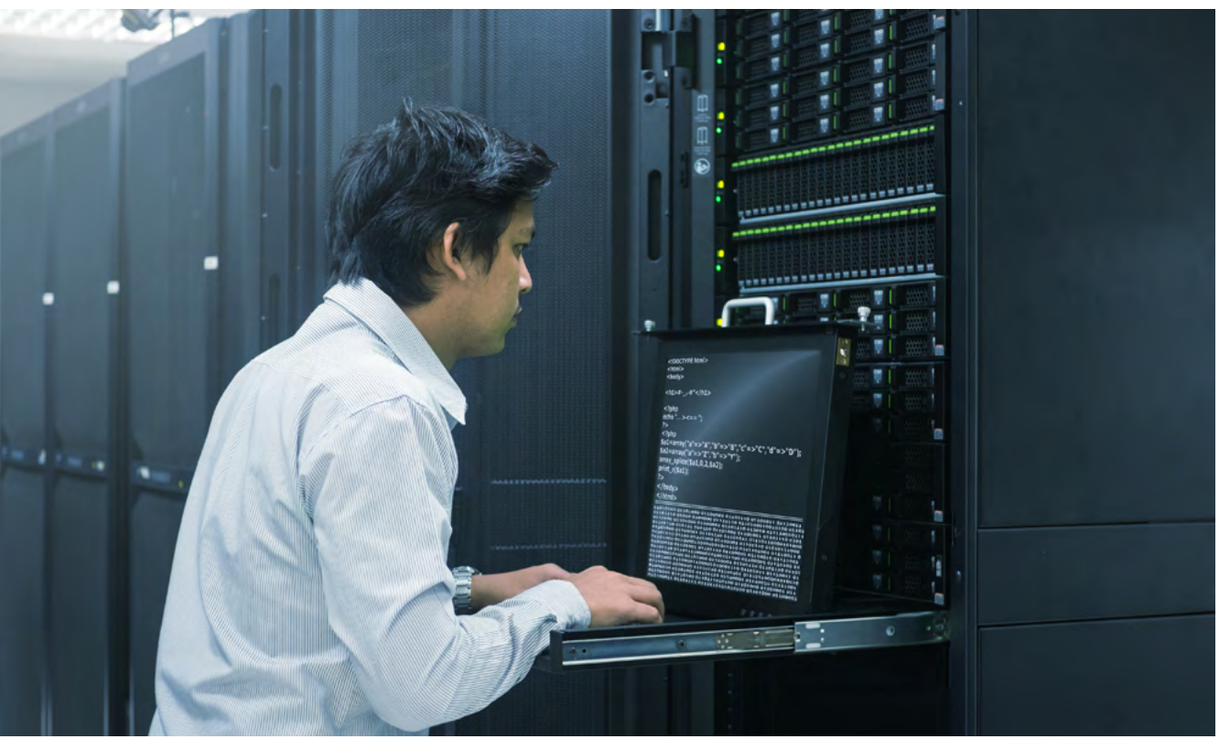
Next

FEATURE

# What Every Enterprise Should Know About Security Product Testing

Test, but verify: With open-testing organizations offering security product testing, companies now have more nonbiased options for evaluating security products for purchase. But you should also take into account your existing security posture.

By Robert Lemos, Contributing Editor, Dark Reading



When Dan Basile looks for new technology to help him secure Texas A&M University System's RELLIS Campus network, his primary considerations are how the equipment performs and whether the product's security lives up to its promises.

As the chief information security officer, Basile wants security technology that can help defend his networks and endpoints against the latest threats, but he worries that marketing promises will not materialize in reality. Unfortunately, no one has time to test each vendor's product for themselves, so the reliance on testing organizations is necessary to make acquiring new systems feasible, he says.

"We only have so many hours in the day, so if someone can take care of the nonbiased work — which is the hard part — of who can meet our initial base requirements, then I can move into the more niche use cases, and I don't have to focus on whether this piece of security equipment protects against a particular class of threats," he says.

Basile is not alone in his desire for nonbiased testing. As companies seek to simplify their security operations and keep cybersecurity costs under control, gauging the performance of security tools and products has become critical. While tools such as the National Institute of Standards and Technology (NIST)'s Cybersecurity Framework

and MITRE's ATT&CK knowledge base are good starting points for companies seeking to cover all their bases, determining whether security products and services meet their needs requires testing that corroborates their vendors' claims.

Delivering that nonbiased — but meaningful — testing, however, has been a struggle for the industry.

Over the past four decades, information technology publications, public and private testing laboratories, and vendor organizations have all tried to provide testing as a service, but the cost and complexity have led many organizations to drop out, while the lack of trust in pay-to-play schemes has undermined the credibility of some providers of testing services.

As a result, a collection of open-testing groups has emerged. Typically a combination of vendors and testing organizations, open-testing groups aim to set the ground rules for security and performance evaluation so that vendors accept the testing frameworks and CISOs can trust the results. One such group, NetSecOPEN, brought together more than a dozen testing labs and network security vendors, creating an open standard for testing next-generation firewalls. Other groups tackling open-testing standards include the Anti-Malware Testing Standards Organization (AMTSO), focusing on endpoint-security product testing, and the public-research corporation MITRE, which creates testing scenarios that line up with real-world threats.

The efforts are a departure from the past, says Brian Monkman, executive director of NetSecOPEN.

"A lot of the reasons why companies try to do the testing themselves is because they feel they can't trust the tests that come out of pay-for-play labs," he says. "We are looking to create a test that is not only open and transparent — which is a too-often-used phrase in the industry — we wanted to take that and actually make it mean something ... because once you can reproduce the test results yourself, you can tweak it in a way that is meaningful for you, and that hasn't existed before."

**Typically a combination of vendors and testing organizations, open-testing groups aim to set the ground rules for security and performance evaluation so that vendors accept the testing frameworks and CISOs can trust the results.**

However, companies need to know the basics of security-product testing, so that they can make the right decisions and get the most from existing testing agencies.

## Consolidation Drives Greater Demand for Testing

Over the past two years, the coronavirus pandemic has changed how businesses operate. Companies moved more of their infrastructure to the cloud, accelerating digital transformations, while at the same time, they have struggled to adapt to the remote-working arrangements that became a necessary part of business during the pandemic. Moving forward, most employees expect to continue to have the option of working from home more often, and that reality means that the challenges in securing enterprise infrastructure will not go away.

CISOs are looking for ways to consolidate their security portfolio, a trend identified before the pandemic but one that has accelerated since. In 2020, more than three-quarters of CISOs had at least 16 security products or tools being used by their security teams, while 12% had more than 45 security products or tools, according to Gartner's CISO Effectiveness Survey. The vast majority of CISOs, 80%, are interested in consolidating their security infrastructure.

Only around 10% of companies, however, currently look at test reports and pilot security technology in their environment to make the right decisions, estimates John Pescatore, director of emerging security trends at SANS Institute and a former analyst at Gartner.

"There is really a goodness around testing in general,

and this whole idea between open test standards," he says. "But only the motivated buyers — the top 10%, which I call the 'lean-forward' guys — only they really use the results to make the best decision."

The rest of companies will forgo testing and instead use analyst reports — such as Gartner's Magic Quadrant and the Forrester Wave — to reduce their options to a handful of products.

Testing organizations should have dual goals, says Pescatore. They need to produce reliable evaluations with the necessary transparency to satisfy large enterprises, while producing easy-to-consume reports so that smaller businesses can decide what tools meet their technical requirements, are interoperable with existing infrastructure, and have the necessary features.

## A Brief History of Testing

In the late 1980s and early 1990s, testing labs emerged as an offshoot of the growth in computer-industry magazines, such as Byte Magazine or PC Magazine, which typically tested a variety of software programs and hardware devices, giving a few Editors' Choice awards. As the products became more complex and magazine budgets shrank, testing companies emerged to better serve companies.

However, vendors began inserting themselves into the testing process, and many testing organizations would specifically run tests for those vendors. Participating in the tests often meant paying the testing organization, and those vendors that did not pay would not be given the opportunity to tune their products for best performance on the tests.

The threat intelligence and testing firm NSS Labs highlighted the issue in 2010s, when vendors began pushing back at the company's business model and questioning nonfavorable evaluations. Following the publication of its results for next-generation firewalls in 2014, Palo Alto Networks took exception to the findings, noting that it did not participate in the test.

**Participating in the tests often used to mean paying the testing organization, and those vendors that did not pay would not be given the opportunity to tune their products for best performance on the tests.**

"The reason we did not participate in this test is that over time we have come to believe that the NSS model of allowing vendor test tuning prior to public test is a 'pay to play' approach and produces questionable objectivity and accuracy in results," the company stated in a blog post.

NSS Labs responded at the time that it treated every vendor's product the same and did not allow tuning. Yet the company's business dried up as the company fought with vendors, which in turn, created organizations that set the guidelines for testing. In 2020, NSS Labs folded, after being bought by a private equity firm.

## The Importance of Open Testing

While any organization could, at one time, run an antivirus scanner on a folder of recent malware or use a vulnerability scanner to test exploits against a firewall, times have changed. One-time private testing organizations with opaque testing protocols and questionable business models have given way to more transparent testing services that have open specifications and transparent processes and are not beholden to specific vendors.

While open-testing organizations are funded by their members — which generally include vendors and testing companies — the groups are not "a pay-for-play business model," says Micki Boland, cybersecurity architect in the office of the CTO at Check Point Software Technologies, which is a member of both AMTSO and NetSecOPEN.

"The testing standards and protocols provide a level

playing field for testing performance standards of security products in catching threats, enabling informed decision-makers to evaluate security solutions based on real testing results rather than the perception of performance," she says.

In the end, someone must pay for testing, but the goal is to make sure that those that are paying do not get preferential evaluations, says University of Texas A&M's Basile. Open-testing organizations not only publish their standards, allowing enterprises to evaluate the testing methodology, but also bring competitors together, which in and of itself limits whether vendors will be able to skew the results.

"There are some interesting power plays with these groups, but you have a lot of competitors who, one would hope, are potentially keeping each other honest," he says. "I'm hopeful that we can see these organizations create open standards that everyone can test against — that makes sense to me."

## Testing, Now Complex, Requires Standards

Take NetSecOPEN. The organization has narrowed its focus on performance of security products under specific security conditions and is in the process of creating a specification for testing network security products through the Internet Engineering Task Force (IETF), which sets all the standards for the Internet. NetSecOPEN first requires the vendors' products meet certain security requirements to mitigate attacks and malware, and then demonstrate that they can do it under load. Once that is done, it locks the configuration and tests the product's performance, according to NetSecOPEN's Monkman.

"This has taken us over four years, and it has been a very difficult process, but kudos to the vendors taking this approach," he says. "As difficult as the process has been, the fact that people are willing to take the time — and remember the majority of the people working on this are volunteers — is because they see the value in this."

The IETF draft is 59 pages long and is on version 13; it probably will require a few more versions before becoming a standard.

By focusing on a narrow set of goals for security testing, NetSecOPEN and AMTSO aim to keep the testing as objective and data-driven as possible, a focus that looks like it will work, says SANS's Pescatore.

"Performance is the natural place to start. It is a better focus because you can't afford to have the security solution be the chokepoint of the network," he says. "There has always been some performance testing, so I think that is a better focus because a lot of time, you cannot afford to have the security solution be the chokepoint."

Yet testing organizations have their work cut out for them just to keep up with the current threat landscape. Between attackers automating the creation of threats to respond to defenders' capabilities and exploring new classes of vulnerabilities, any specification must be flexible to deal with the fast-changing ecosystem, says John Hawes, chief operating officer at AMTSO.

"Testing the efficacy of security products is extremely difficult, mainly because we are dealing with a constantly changing environment," he says. "You can't look at the threat that is attacking you today and say, 'As long as I test every day and this threat is being blocked, then I will be fine.' It will be a different threat tomorrow and a different one next week, and in 10 days' time, all the threats you were looking at will be history and forgotten about."

**Open-testing organizations not only publish their standards, allowing enterprises to evaluate the testing methodology, but also bring competitors together, which in and of itself limits whether vendors will be able to skew the results.**

## Companies Need to Evaluate Based on Their Threats and Infrastructure

By considering the input from multiple parties, open-testing specifications have a better chance of accounting for current threats. In addition, security-product evaluations that conform to an open standard can give companies and their CISOs a more reliable way of gauging whether a specific security product will work with their existing infrastructure and performance demands.

To take these considerations into account, testing companies have moved beyond setting up hardwired test environments to software-based tests and virtual networks to create a "digital twin" of a company's network and operational infrastructure, says Sashi Jeyaretnam, senior director of product management for security solutions at testing-solutions provider Spirent.

"Testing has evolved toward more of software-oriented test agents that are deployed to be able to represent a realistic enterprise network, like a digital twin or a predeployment version of the enterprise network," she says. "It is not only about security effectiveness but the quality of the end user's experience, as well as the security efficacy in conjunction with a particular environment."

With some product categories, testing specific functionality makes sense. Companies want to know whether an anti-malware product blocks the threats they are seeing, or that a next-generation firewall will inspect traffic for security threats while it's handling peak throughput.

However, many times a corporate executive hears about a specific cyberattack in the news and wants to know if their company would have fared better against the adversary than the victim did. In some ways, that's the approach that MITRE has taken with its ATT&CK Evaluations, with exercises aimed at reproducing the common steps seen in specific campaigns or types of attacks.

**"You can't look at the threat that is attacking you today and say, 'As long as I test every day and this threat is being blocked, then I will be fine.' It will be a different threat tomorrow … and in 10 days' time, all the threats you were looking at will be history and forgotten about."** —John Hawes, AMTSO

Perhaps best known in the cybersecurity world as the creator and manager of the Common Vulnerabilities and Exposures (CVE) database, MITRE has also created the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, which categorizes attackers' methods and tactics. Basing the discussion on real-world adversaries described by the ATT&CK framework gives companies a different way to look at their security infrastructure, says Jamie Williams, principal adversary emulation engineer for MITRE.

"The beauty is that it is kind of a 'Choose Your Own Adventure,'" he says. "A lot of companies will go in and look at particular vendors and decide if they are the right fit. Other companies are looking at the reports to gather information and see what really matters to them."

Using test reports to learn about the approaches of specific vendors to a security problem is also an advantage of open testing. Looking at the historical performance of a company in tests speaks to the reliability of the vendor, and companies should use test reports to research potential vendors, says AMTSO's Hawes.

"Try and get as much data as possible," he says. "If you are considering making a purchase, do your research, find out what tests those vendors have been included in, and monitor the vendors over time as well — look back maybe a year or so. A single point in time is only a little snapshot, and what you need to know" is if it is consistently good.

## The Future of Testing

While testing organizations are standardizing testing methodologies, the business world is starting to change. The pandemic has turned "digital transformation" from a

buzzword to an essential survival skill. Ninety-two percent of companies plan to use multiple clouds to run their business, while 80% will keep some on-premises technology as well, according to Flexera's 2021 "State of the Cloud Report."

This push to cloud has already affected security products. Continuous testing and attack surface management has become aspirational goals for many companies, although only a few have the depth in their security teams to realize that goal today, says Jon Oltsik, senior principal analyst at the Enterprise Strategy Group.

"Aggressive users of the technology are doing just that," he says. "If there is an aggressive ransomware attack and the board asks, 'Are we protected?' — in a perfect world, the security team would be able to answer, yes, we are, or no, we are not. The model is there, and it is sound, but only for bleeding-edge organizations."

The testing organizations are adapting to that future as well. AMTSO, for example, is working to create standards for protecting Internet of Things (IoT) devices. The University of New Hampshire's InterOperability Lab (UNH-IOL), a founding member of NetSecOPEN, is watching the evolution of business operations in the cloud to evaluate how that shift changes testing.

Because the environment is changing so quickly, the shift will change testing and require continuous training to remain on top, says Timothy Carlin, senior executive for software development at UNH-IOL.

"Folks are still buying firewalls, and that is not going to change anytime soon, but there are some places that will go to cloud-only offices ... and that move to cloud is interesting and it's something that we are keeping our eye on," he says. "Because there is a whole new world there with massive cloud deployments, I still don't think we fully understand what it will take to protect them."

In the future, testing needs to be more pervasive and more open. Companies should not just rely on open-testing organizations to gauge the reality behind the marketing data sheets produced by vendors, but also make testing part of their own security operations, says Texas A&M University System's Basile.

Testing the security performance of a specific product only gives an idea of the potential of the product. Holistic testing — through attack surface management or on cyber ranges — on a regular basis will allow companies to determine if the security product continues to work as advertised and whether it continues to protect the infrastructure in the way it should.

"We need to be doing real-time testing of our holistic systems, not just using security tools — hopefully, that will solve some of those issues or at least help you find them," Basile says. With open-testing organizations, trusting the test becomes a bit easier, but companies should still verify their security on their own network.

**About the Author:** *Rob Lemos is a contributing writer at Dark Reading. He is a veteran technology journalist of more than 20 years and a former research engineer. He has written for more than two dozen publications, including MIT's Technology Review, Popular Science, and Wired News.*

## Security Testing Organizations

A variety of groups are trying to create open-testing frameworks and thread the needle between testing organizations and the vendors whose products they evaluate.

### Anti-Malware Testing Standards Organization (AMTSO)

Established in 2008 to improve the quality of the performance testing of anti-malware solutions, the group has produced a testing protocol standard and created the Security Features Check (SFC) tool to confirm that endpoint protection solutions are properly configured. AMTSO's 26-page "Testing Protocol Standard for the Testing of Anti-Malware Solutions" focuses not only on the testing methodology but also prescribes the necessary protocols for contacting the vendors and establishing a dialogue.

### MITRE's ATT&CK Evaluations

MITRE is a nonprofit corporation focused on research and development to support the US government. Using the framework, the company has performed yearly evaluations of different IT configurations against known adversaries. In 2022, MITRE plans to evaluate managed service providers, but past evaluations included detecting how industrial control systems fared against the Triton group's tactics and how a plethora of endpoint protection systems fared against criminal ransomware and nation-state operations using wiper programs.

### NetSecOPEN

Starting with 11 founding members in 2017, NetSecOPEN aims to create testing standards for network security devices. Now with 14 members, including two test labs, three test-solution providers, and nine network-security firms, the group is close to establishing the first network-security test standard.

NetSecOPEN's proposed standard focuses on how to test, not what to test, so that any company can test the same product using the standard and get comparable results. While the organization has started by creating specifications for testing next-generation firewalls, the group plans to move onto other network security devices in the future. ***—Rob Lemos***

## Making a Standard

Four years, 13 versions, and likely a few more to go.

NetSecOPEN's quest for an IETF standard started with its first submission in 2017 — draft 0 — and continues today. The group has submitted its specification, "Benchmarking Methodology for Network Security Device Performance," for configuring testbeds, system- and devices-under-test (the SUT and DUT, respectively), and the test equipment, as well as creating standardized vulnerability sets and operating the various elements of the network. The proposed standard also specifies the test procedures, the expected type of results for each test, and the information that a test report should contain.

Among the specified tests for network security devices, for example, are the throughput performance using specific application traffic mixes, the number of TCP or HTTP connections that the device can handle per second, and the HTTPS throughput.

The goal of the standard is to create a minimum level of transparency for future tests, says Brian Monkman, executive director of NetSecOPEN.

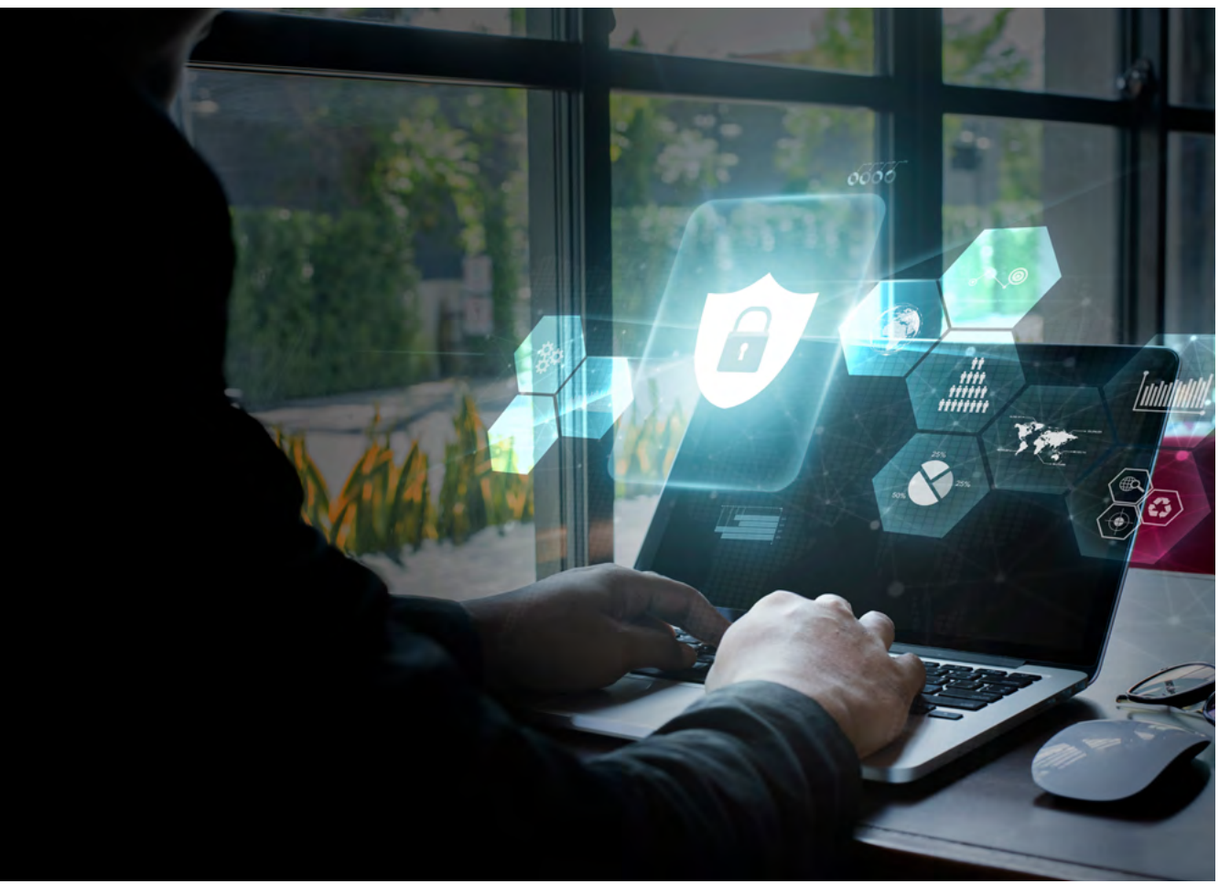
"There is no way that any one test is going to be able to satisfy multiple enterprises," he says. "So we are looking to create a standard that is not only open and transparent — which is a too-often used phrase in the industry — but we wanted to take that and actually make it mean something." ***—Rob Lemos***

NetSecOPEN PERSPECTIVES

# From the Desk of the Executive Director of NetSecOPEN

What to expect from the open, security product testing organization — and how to get involved.

By Brian Monkman, Executive Director, NetSecOPEN



It has been an up-and-down few years since the inception of NetSecOPEN as a nonprofit, membership-driven organization. Our mission has not changed. It remains "to work with industry and others to create well defined, open, and transparent standards that reflect the security needs of the real world." Additionally, our vision is to create a testing program that would offer participants multiple choices of test tools and test labs with the reassurance that the test results will be comparable, regardless of which tools and labs they choose.

Working with the NetSecOPEN membership has been both a pleasure and incredibly humbling. The pleasure, in part, is seeing competitors come together to develop test specifications and test methods. Parking their competitive spirit at the door, so to speak. The humbling part is seeing the idea we had start to bear fruit.

That isn't to say that it has all been smooth sailing. Obviously, the pandemic has brought its own challenges. But the greatest challenges have been in the creation of traffic mixes, exploit and malware test sets, and evasion techniques. It was easy to agree on the "what" — much different when it came to the "how." It isn't enough to make sure the right stuff is added to the test tools and just push play with the expectation that everything will line up. Every test tool generates traffic differently by default. Of course, this means that testing results can be, and usually are, very different when using the default configurations of the test tools. Fortunately, the test tool vendors are working to close this gap. It will never be exact, but it will be very close.

Our goal is to begin testing with the malware-, exploits-, and evasion-technique test sets as well as their test methods, plus implement security testing under load requirements, in the third quarter of 2022. This is in addition to the performance requirements detailed in the draft RFC. The malware and exploit test sets consist of thousands of unique samples. We plan to update sets at least once a year.

The test and certification reports will always be public and available for download at no charge. Additionally, security vendors are required to provide NetSecOPEN with the configuration files of their product we test. This is then available to anyone when requested. The goal is to ensure that anyone with familiarity on how to use the test tools will be able to reproduce the test results.

In the following columns by NetSecOPEN members, you will find information that expands on what I have discussed above. One column details the certification process. Another predicts that the disappearance of the physical network perimeter and increased migration to cloud-based security will require testers to expand their offerings.

We believe that this prediction is accurate. You already see most security vendors well-known in the network security sector now offering Azure-, GCP-, and AWS-native versions. While the security and performance requirements enterprises demand will not be the same, the manner in which these products are tested will be both different and challenging. But there still will be the need to create test requirements and methodology that are transparent and open to input.

What NetSecOPEN needs is a wide range of voices at the table, and enterprise involvement is key to the long-term viability of this effort. What enterprises want and need must be reflected in the work we undertake and the results of those efforts.

NetSecOPEN membership is open to anyone who wishes to actively participate in these efforts. If you are interested, or know someone who is, please feel free to email me at bmonkman@netsecopen.org

**About the Author:** *Brian Monkman is Executive Director of NetSecOPEN, a nonprofit, membership-driven organization with a goal of developing open standards for testing network security products. A 25-year network security veteran, he has extensive experience in technical support, sales engineering, and program management roles at technology companies including Nortel Networks, ICSA Labs, Sterling Software, and others. At NetSecOPEN, he leads an effort to significantly change network security product testing by developing open and transparent testing standards that will be used by approved test labs to test network security products in a manner that produces verifiable and repeatable results.*

# Impact of Neutral Agencies in Evolution of Security

NetSecOPEN's framework can pivot to other security product tests in the future.

By Amritam Putatunda, Senior Product Manager of Application & Security, Keysight Technologies

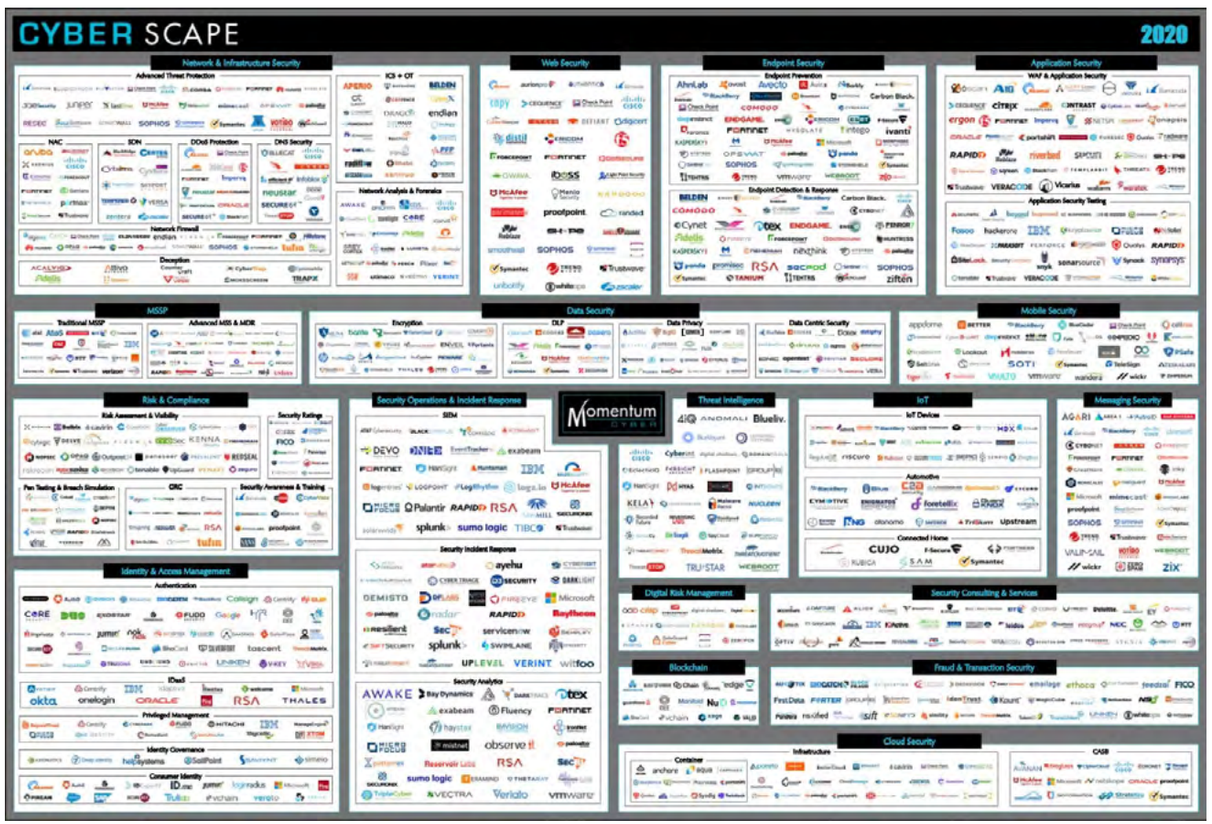



Figure: Are we safe yet

Security is a journey and not necessarily a destination. Which means we are trying to continuously be better in securing assets without a particular end in sight. The last few years have shown how the attackers have leveraged the perimeter-less ecosystem, such as the advent of smart devices, Internet of Things, etc. to their advantage by gaining access to some of the most reputable organizations in the world. Every security vendor is contributing to this journey where they rapidly adapt modern technologies to counter the security threats of this ever-growing rapidly changing internet ecosystem. This has also allowed newer products, features, and functionalities to be rolled out into the market. Capabilities like zero trust security, secure access at service edge (SASE), XDR, cloud security, software defined perimeter, etc. They are also fortifying features within their existing infrastructure to allow better security controls and quality of experience like rapid adaption of HTTP2 and now HTTP3, enabling TLS1.3 for man-in-the-middle deep packet inspections, integrating 3rd party identity providers for better authentication, etc.

## The Problem with Security

We would like to believe every vendor is diligently working to get the right products with the right features to the customers. However, we also must look at the precarious position that the consumers are in when they have to choose from

an explosively expanding list of cybersecurity vendors, each promising their product to be better than the next in solving their security concerns, with their data sheets claiming superlative performance numbers and even better security efficacies.

## Why an Independent Agency for Security Evaluation?

As mentioned, even though products or technologies may be different, their objective is still the same: securing assets while maintaining quality of experience. That's why an independent authority can be extremely useful in this case. Every vendor has responsibilities to its company, shareholders, and its people to maintain profitability and hence has a vested interest in pushing their products. But an independent nonprofit isn't bogged down by those same constraints. By its very design, it can't take sides and doesn't have specific vested interests, and its only agenda is to provide information to the consumers so that they can take the decisions that's right for them.

## Eliminating Biases in Test Methodologies — A Guiding Force for NetSecOPEN

The objective of the NetSecOPEN test methodology has been clear from the get-go. We knew there was a huge gap in the security market — that is, providing a neutral perspective. We just had to design a test methodology framework that's free from as much bias as possible. A methodology that would represent most common consumer use cases, a methodology that would cover both application performance and network security, and most importantly a methodology that can be run by variety of test tools against a variety of devices. A major portion of effort has gone into eliminating biases that are either ingrained in people or in their beliefs. However, as a collaborative forum, these efforts are ongoing and we are getting better as a group in getting rid of our company-specific agendas to come together for the collective betterment of the industry.

## The Journey Has Just Begun

NetSecOPEN intentionally chose the next-generation firewall (NGFW) as the first methodology because it was already at a certain state of maturity and has found its place in the world of security. Next-generation firewalls are also feature rich as they can cover a variety of functions, like application policing and control, URL filtering, malware/spyware detection, deep packet inspection, etc. Hence, building a robust framework that builds tests methodology to validate security efficacy and performance for NGFW gives NetSecOPEN a perfect launch pad to quickly pivot to other upcoming areas like cloud security, Secure SD-WAN, ZTNA, endpoint detection, etc.

The biggest challenge that we may face in testing such new technologies is to create specific topologies. For example, cloud security would need deployment of traffic generators in the cloud, and SD-WAN would need distributed locations. But the framework NetSecOPEN has built means only incremental changes in terms of applications or attack profiles, will be needed to independently test such technologies and determining their efficacies as an individual product or a combined solution.

**About the Author:** ***A cybersecurity specialist, Amritam Putatunda supports the development and management of key products within Keysight's security portfolio. He has been in the test and measurement industry for the past 16+ years.***

SONICWALL PERSPECTIVES

# NetSecOPEN Ushers in New Era in Cybersecurity Testing

Additional standardized testing requirements are in development, but testing standards for network firewalls have been completed and a few vendors have been certified.

By Aria Eslambolchizadeh, Vice President, Chief Security Officer, SonicWall

Because so much depends on an organization's cybersecurity solution, the ability to make apples-to-apples comparisons is crucial. However, doing so has traditionally been difficult. Vendors tend to report results obtained under the most favorable conditions, making it difficult to tell how close these results are to real-life use.

Even third-party testing companies, which bill themselves as independent, use proprietary and closely guarded testing methodologies and criteria. Moreover, the results and interpretations are not independently reviewed. Since test criteria and methodologies vary widely from lab to lab, buyers have little means to discern how a solution would function in their own networks.

NetSecOPEN was formed in 2017 to help close this gap between proprietary performance metrics and the actual observed performance of security solutions. This nonprofit organization brings together leading security vendors, testing solutions and services vendors, testing labs, and enterprises with the goal of creating open, transparent network-security performance testing standards. These standards are based on fully configured, realistically deployed security solutions and provide guidelines and best practices for testing modern network infrastructure.

Unbiased and independent testing is a core component of NetSecOPEN. The organization provides guidance for interpreting results, oversees the creation and updating of standards, and oversees evaluation testing. The testing strategy has been designed by

most of the top 10 cybersecurity vendors, including SonicWall, Cisco, Fortinet, Juniper, Palo Alto, and Sophos, as well as testing equipment vendors Keysight and Spirent and testing labs EANTC and UNH-IOL. This ensures that the tests don't favor one vendor over another.

And because NetSecOPEN testing labs are subjected to regular competence reviews, the testing process itself is assured to be independent and conducted according to stated guidelines. The entire process is conducted openly and transparently, with meetings recorded and project status posted on the NetSecOPEN website.

NetSecOPEN testing isn't just standardized and transparent — it's comprehensive as well. NetSecOPEN is working with the Internet Engineering Task Force (IETF), the premier Internet standards body. The IETF is an international community of network designers, operators, vendors, and researchers, all concerned with the evaluation of the Internet architecture and the smooth operation of the Internet.

NetSecOPEN's open standardized testing, which is in the process of being adopted by the IETF, measures criteria such as HTTP and HTTPS throughput, connections per second for TCP/HTTP and HTTPS, transaction latency for TCP/HTTP and HTTPS, and concurrent connection capacity for TCP/HTTP and TCP/HTTPS.

While testing against these standards can be conducted by anyone, only certified labs are allowed to perform certification testing.

To become certified, a product vendor first must enter into a testing contract with a NetSecOPEN-approved test lab. Once testing is complete, the test lab provides the product vendor with the testing reports for review. A product vendor may elect at any time to withdraw a product from testing, and it can ask the testing lab to redo some tests. But to maintain transparency, the testing report documents any redone tests as such.

Once the vendor has examined them, the test reports are sent to the NetSecOPEN certification body for review. The certification body can ask the test lab and/or product vendor for clarification of the results, and it may ask that some tests be redone or that another approved test lab conduct a spot check.

When the results are approved, NetSecOPEN creates a certification report, which includes an overview of the test results, including information on the device being tested, such as device model, firmware build/product version, a copy of the device configuration, and test tool information, along with the configuration of the test tool. NetSecOPEN then awards the certification and publicly reports the results.

While additional standardized testing requirements are in development, the testing standards for network firewalls have been completed, and a few vendors have already been certified, including SonicWall.

The SonicWall NSa 4650 was certified by NetSecOPEN at 3.5 Gbit/s of threat protection and up to 1.95 Gbit/s SSL decryption and inspection throughput, suitable for data center use.

To learn more about the SonicWall NSa 4650, click here.

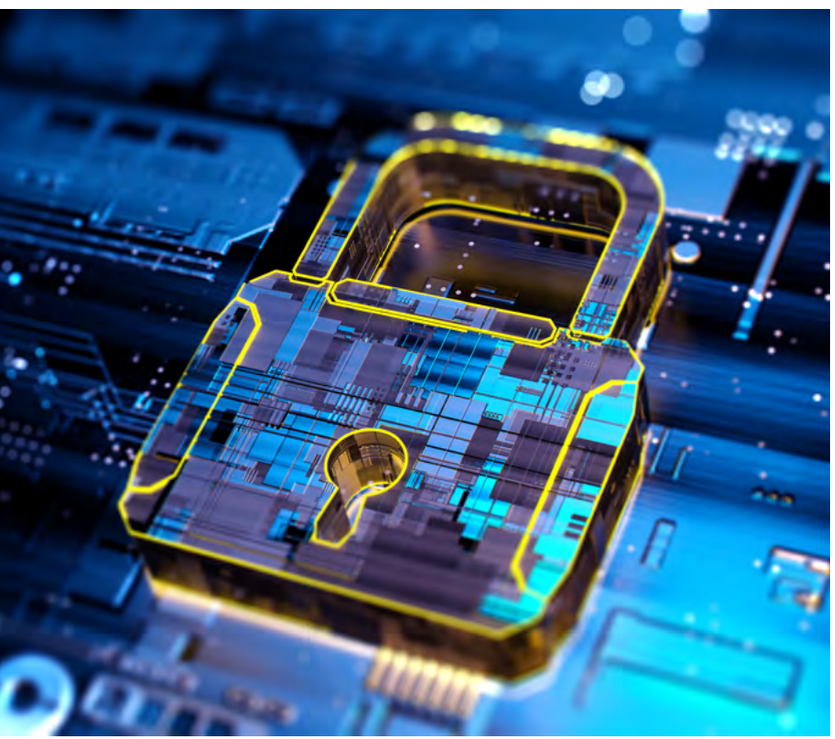
**About the Author:** *Aria Eslambolchizadeh is Vice President at SonicWall, responsible for Corporate Security and Quality Engineering. Aria started as a Software Developer at BNR, which was acquired by Nortel Networks. He spent over a decade working within R&D on enterprise and carrier products. Aria held various R&D leadership roles working in France, Ireland, Canada, and the USA, gaining valuable perspectives on different products and cultures. Aria joined SonicWall in 2003 managing a small Quality Engineering team, growing the organization to over 130 Quality Engineers working across the solution portfolio. Aria holds a Bachelor of Electrical Engineering from Concordia University, Montreal, Canada, and holds multiple U.S. patents related to VoIP and network security.*

SPIRENT PERSPECTIVES

# Let's Get Real: Network Security and Performance Testing Needs to Be Open to Evolve

For products and services to evolve as quickly as the security landscape — with full trust and confidence in test results — look to open, collaborative, objective approaches such as NetSecOPEN.

By Michael Jack, Director of Operations, Spirent Security Solutions



We've got two words for anyone still arguing that network security and performance testing should be performed by independent firms using proprietary test suites:

Things change.

Consider just a few of the changes that have impacted the security landscape in recent years:

- The data center is no longer a "center"
- The corporate network is now a massive web of networks
- The perimeter has been distributed to the edge
- Every user is now a remote branch office
- Encryption has gone mainstream
- Cloud apps have become pervasive
- Mobile device users are adopting 5G in droves

Architectures and equipment continue to evolve as well. New approaches such as secure access service edge (SASE) and zero trust are quickly replacing SD-WAN and previous-generation architectures. Next-generation firewalls (NGFWs) are now supporting dedicated antivirus (AV), intrusion detection systems (IDSs), intrusion protection system (IPS) engines, and much more to expand their effectiveness and meet today's requirements.

All this change adds complexity and difficulty to assess and validate performance, quality of experience (QoE), and security efficacy of these solutions. The key question today is: What is the best way to make sure testing keeps pace with change?

Independent testing with proprietary test suites has consistently failed on multiple levels. Many labs use proprietary tests and methodologies that lack external scrutiny and transparency; they are not standardized, so they can't

provide objective, apples-to-apples comparisons. So, while change continues to accelerate, trust continues to evaporate between equipment vendors and test firms.

The root problem is that proprietary tests are inherently slow to adapt to fast-changing risks and modern IT realities, and in some cases they favor the capabilities of one device over another. A community approach — based on open standards and realistic testing using certified Common Vulnerabilities and Exposures (CVEs) scenarios, performance methodologies, and traffic mixes — is the only way to provide relevant results and trustworthy guidance on network security and performance, because it is the only approach that is capable of evolving quickly enough.

Why does openness lead to faster evolution of network security testing and validation? Several key factors are at play:

- Communities provide multiple sources of knowledge, expertise, and ideas. This enables testing methodologies to evolve quickly based on today's real-world threats, traffic types and patterns, market conditions, and more. That's the reason NetSecOPEN was formed in 2017. Since then the organization has grown and evolved quickly, thanks to the contributions and active participation of more than a dozen network security leaders, who have jointly created open testing standards recognized by the Internet Engineering Task Force (IETF).
- In addition to the NetSecOPEN IETF Benchmarking Methodology for Network Security Device Performance standard, the NetSecOPEN forum is evolving test suites to include broader test coverage, mixed-traffic performance testing and validation, a pathway to cloud-based validation and security efficacy, standards for benchmarking vendor performance, and much more. NetSecOPEN has also expanded its testing capabilities with the upcoming addition of new security assessment tests, growing from 400 attack scenarios in 2017 to thousands today, enabling vendors to validate an ever-widening array of devices in realistic conditions.
- Openness facilitates continuous improvement in product engineering. By using test results from open communities, vendors can continuously evolve their products in response to fast-changing security landscape and market conditions. For example, they can test their products against the NetSecOPEN test suite in their own labs at any time, which allows for more agile product improvement by incorporating more frequent internal performance testing. This can also reduce the cost of optimizing products to perform well in independent tests.
- Real results expedite innovation. With an open, community-based approach, vendors can quickly get beyond "vision" and make sure their innovations really work. Thus, they can answer core questions faster: Is the new SASE/cloud architecture truly delivering the level of security and performance your customers expect? What is the impact of variations in the traffic mix on security risks and overall performance of distributed networks? To answer such critical questions, vendors and network operators can easily evolve and extend the NetSecOPEN methodologies to cloud infrastructure to assess the security and performance priorities of their specific business workloads.

Let's get beyond the idea that proprietary test suites are a valid option for security and performance validation. If you want your products and services to evolve as quickly as the security landscape — with full trust and confidence in the test results — look to open, collaborative, objective approaches such as NetSecOPEN. At Spirent, we believe great ideas come from everywhere, and great ideas should be shared.

**About the Author:** ***Michael Jack is Director of Operations – Spirent Security Solutions Communications' applications and security solutions portfolio. He has 20 years of working in the data communications industry and over 15 years working for networking test and measurement organizations. At Spirent Communications, Michael works with the Product Management team to define, produce, and deliver cutting-edge applications and security testing solutions for network equipment manufactures, enterprises, and services providers. Michael has presented at numerous industry events and has worked in product marketing and management capacities at a diverse number of networking companies, including Thomas-Conrad, UB Networks, Newbridge Networks, Compaq, and Antara.***

UNH-IOL PERSPECTIVES

# Piecing Together the Performance Testing Puzzle

NetSecOPEN is developing more security effectiveness test cases as it works to expand and evolve its consensus-driven testing model.

By Tim Carlin, Senior Executive, Software Development, UNH-IOL | Chris Brown, Technical Manager, Routing and SDN, UNH-IOL

Performance testing for networking and data communication products has long been a subject of interest, conflict, and confusion. When compared to compliance or interoperability testing, performance testing methods may be the most well-known: For example, there are many applications and tools for measuring the speed of a device or a network, or to detect network problems. However, these tools tend to be focused on a singular metric, and they don't necessarily consider variations in configuration, environment, or network conditions. This leads to a useful test in isolation. But when used for comparisons, the results are usually not portable.

Compliance testing has the obvious benefit of consensus-backed statements for correct and incorrect operation, including protocols, packets, and bytes. Interoperability testing relies on the straightforward question "Do the products work together or not?" With performance benchmarking testing, it would seem just as straightforward — a device should meet or exceed the performance represented on the product's datasheet. But we are then faced with questions: How is it determined what is "good" or "great?" Is that definition consistent? What about when we compare products? Devices within the same product line have different design targets. Even though most next-generation firewalls (NGFWs) and next-generation intrusion prevention system (NGIPS) devices have similar capabilities, the implementations differ. This grows orders of magnitude more complex when considering competing products.

So let's explain how these security product performance questions have been addressed today, and what additional testing components are coming in the near future.

## Building NetSecOPEN

Since 2017, NetSecOPEN has been answering these questions and challenging the industry to not only set the bar, but to raise it. Borrowing a page from the compliance testing handbook, NetSecOPEN brought together industry experts to develop a consensus-based specification — Benchmarking Methodology for Network Security Device Performance — that covers both NGFW and NGIPS devices. More than two years after the launch of the program, more than nine products have been tested against the specification and received published certification reports, serving the mission of developing open, standardized tests based on real-world network conditions that enable an apples-to-apples product comparison.

However, publishing the NGFW Performance RFC is only one piece of the puzzle. Additional testing methodologies are well on their way toward adoption and formal certification testing. NetSecOPEN is currently working on implementing new security effectiveness test cases as well as traffic mixes with applications commonly used in various industries (healthcare, education, etc.).

This ongoing development demonstrates the true value of NetSecOPEN, which represents an ecosystem of members such as security product vendors, testing solution and service providers, testing labs, and enterprises. NetSecOPEN also creates an environment in which processes, standards, and technology can be discussed openly, transparently, and collaboratively. A sustainable cycle has been built where product vendors and enterprises drive technology innovation, tool vendors develop insightful measurement applications, and test labs like University of New Hampshire InterOperability Lab (UNH-IOL) provide a neutral evaluation. However, this evaluation is not the terminal state: The information gleaned from in-lab testing is used to inform development of the standards, to enhance the tools, and of course to improve the operation of the security products themselves.

## Harnessing the Potential of Cooperation

As more products are tested and certified, the value of the NetSecOPEN program will become clear to both enterprises and end users. Its ultimate goal is to inform, educate, and provide a clear understanding of differences between products. With this kind of understanding, enterprises will be able make purchasing decisions that align with their needs more quickly, easily, and effectively.

However, those needs might not be easily discernible from reviewing the certification results. In those cases, the openness of NetSecOPEN allows the organization to bring those gaps back to the industry. Enterprises that find areas where additional testing or different metrics would be valuable can participate in, and build consensus among, a working group of peers with the common goal of improving the state of the technology.

In the end, the extent to which NetSecOPEN — or any certification program — is successful depends on all stakeholders getting involved in a way that removes competitive barriers and focuses on the technology. Additionally, it requires representation from all points of the pipeline, from early product development to user adoption. The true potential of NetSecOPEN will only be realized with input and feedback from all of these phases in a consensus-driven manner.

**About the Authors:** *Timothy Carlin, Senior Executive, Software Development, UNH-IOL. Tim is the technical lead for all IPv6, Routing, and Security-related testing and development activities at the laboratory. He is involved with the development and maintenance of the USGv6, IPv6 Ready Logo, and NetSecOPEN testing programs. His current role also includes planning and guiding the organization-wide IT and Software strategy.*

*Christopher Brown, Technical Manager, UNH-IOL. Chris is the technical manager for the Routing and NetSecOPEN testing services. He has extensive knowledge of routing protocols including BGP and OSPF. He has developed conformance test solutions utilizing the IOL's custom software, IOL INTACT®.*

VIAVI PERSPECTIVES

# NetSecOPEN Opens Up Security Test Standards

Next-generation firewalls are the first product category the organization is testing.

By Anand Vijayan, Product Manager, VIAVI Solutions

Until recently, the certification of security product performance was a decidedly mixed bag. The process was typically conducted by independent testing laboratories using proprietary testing methodologies. Since the methodologies and test criteria differed from lab to lab, many proprietary methods to determine performance were in play, and like-for-like evaluation of security products was difficult for enterprise buyers. And, without the ability to compare solutions on a measure-for-measure basis, it is difficult to be sure that a security solution performs the same way in a customer environment as it does in a lab.

The not-insignificant shortcomings of the prevailing security-system performance testing landscape were squarely redressed in 2017 with the formation of NetSecOPEN, a nonprofit, membership-driven organization developing open standards for testing of network security products.

NetSecOPEN was established to tackle the pressing need to have transparent, open tests of the performance impact of security solutions in real-world conditions that could be fully compared with other security solutions. Its founding members are some of the world's leading security product vendors, test equipment vendors — one of which is VIAVI — and testing laboratories. NetSecOPEN's initial focus is on next-generation firewalls (NGFWs). This was an appropriate area on which to begin to focus, as many organizations at that time had little understanding of what effect an NGFW would have on a network.

The resultant NetSecOPEN testing standard was developed jointly by its members. The standard features a real-world mix of traffic, including 400 encryption certificates and 10,000 unique URLs. This unique real-world aspect of the testing methodology provides a more accurate picture of the load performance that security products encounter.

One solution accredited for use with the NetSecOPEN NGFW test methodology is TeraVM from VIAVI. This is a virtualized software-based L2-to-L7 test tool running on off-the-shelf hardware and in the cloud.

## Future of Security Testing

We are presently witnessing a dramatic transformation of enterprise networking and its associated security environment. This change is being driven by major and ongoing public and private "cloudification" of business and workplace activities, combined with the growing use of personal communication devices, increased personnel mobility, and the COVID-generated boost to remote working.

From a security perspective, traditional enterprise premises-oriented network defense perimeters are weakening and disappearing. The upshot is that the need to revisit existing and probable, latent security vulnerabilities is becoming more and more urgent.

## Testing Security in the Cloud

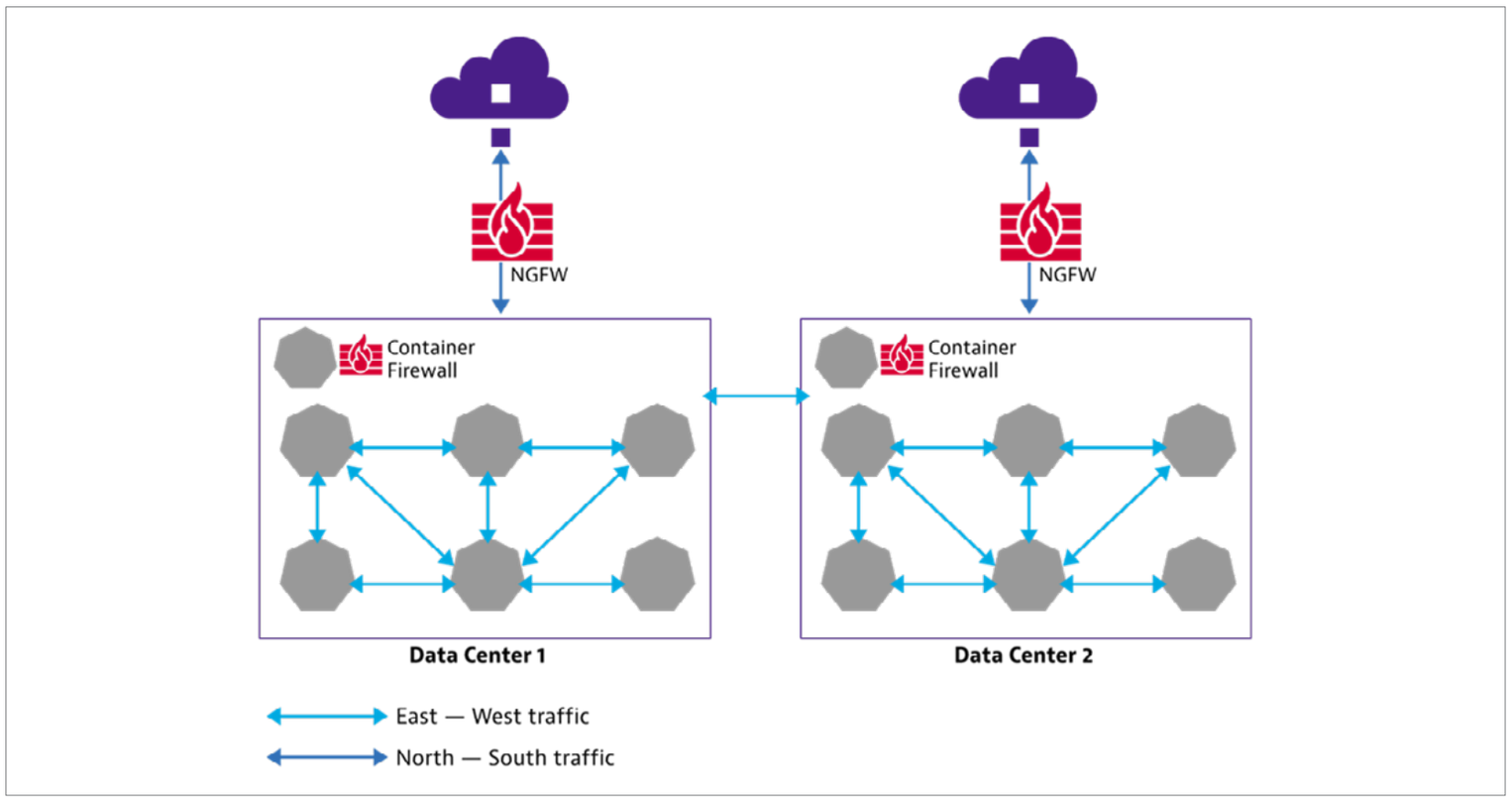
Validating NGFWs that are distributed and span multicloud infrastructures requires a tool that has similar capabilities. In this context, TeraVM is a software-based, virtualized, and containerized NGFW and network validation tool that runs in labs, data centers, and the cloud. The same features and interfaces are available on multiple platforms — data center, cloud, or on-premises. Additionally, TeraVM components can be deployed in a distributed and hybrid network with central control.

NGFWs, meanwhile, also are evolving to be deployed in container clusters in the cloud, and this is where challenges can arise.

Container-based microservices are typically ephemeral workloads that are constantly started, stopped, and updated through CI/CD pipelines. As containers scale horizontally and grow faster, there is an explosion of the east-west traffic — what is called internal traffic — within the container clusters. Traditional firewalls and NGFWs that offer protection at the edge for external/north-south traffic are unsuited for securing container, traffic as they do not "see" them.

As such, container security requires a different approach. A container firewall offers east-west as well north-south protection in a cloud-native environment. You need a cloud-native firewall to protect cloud-native container traffic. Similarly, you need a cloud-native test tool — with visibility to the internal cloud network — to validate cloud-native firewall solutions, by emulating east-west pod traffic.

The VIAVI TeraVM product is a commercial tool that offers a cloud-native testing solution. The TeraVM testbed



is a group of TeraVM components that generate IP test traffic with customizable traffic profiles. Users can deploy the tool using Helm Package Manager in Kubernetes environments hosted on the public cloud, and it can be deployed — and traffic generated — without any third-party network plugins. TeraVM supports a variety of voice, video, and data traffic profiles that can be emulated in the container network. Traffic is generated between TeraVM client and server pods using Service Ips, and the capacity of the testbed can be scaled by deploying more TeraVM pods. This allows users to validate containerized firewalls for TLS traffic inspection, URL filtering, and custom threat generation.

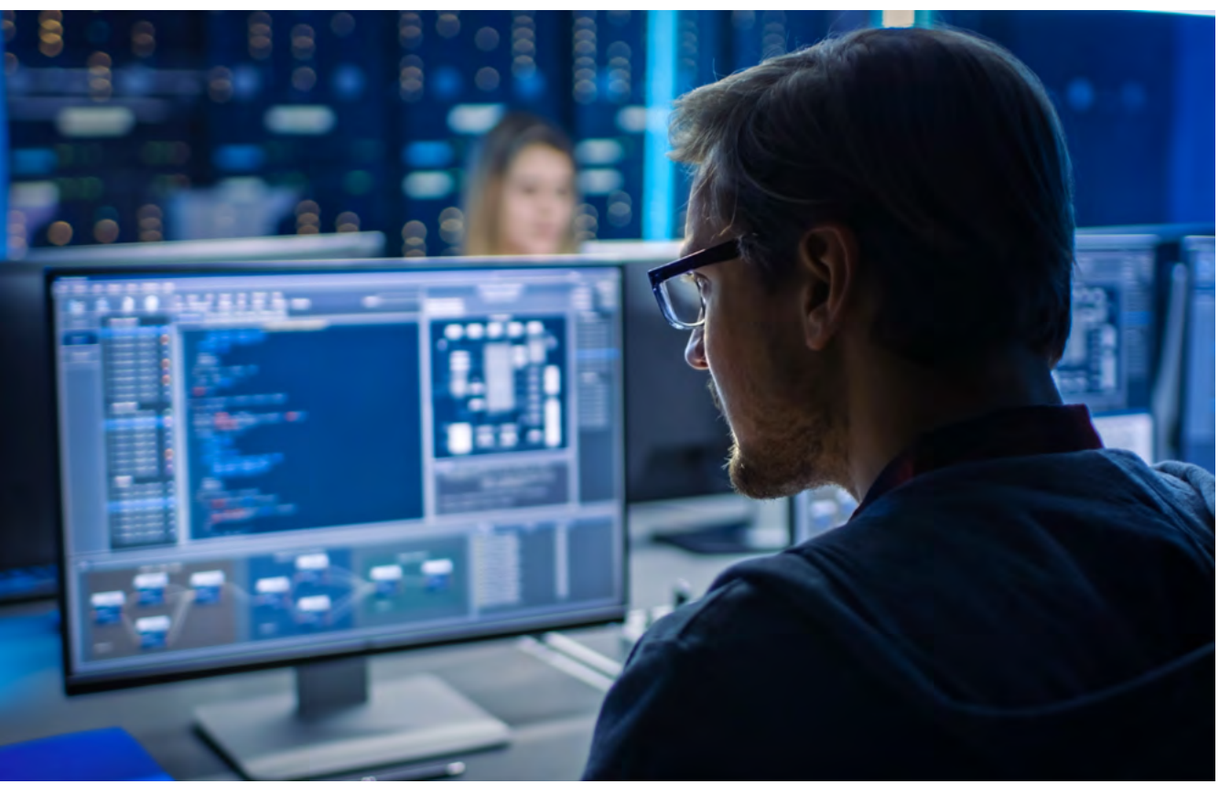
We've grown accustomed to virtual environments and cloud-native applications and the benefits they bring to developers, enterprises, and end users. It makes sense that we take the same approach to network and security testing: using cloud-native security testing tools.

**About the Author:** ***Responsible for product management, strategy, and new product introductions in the VIAVI Solutions Wireless Business Unit, with particular emphasis on TeraVM family of products which provides NGFW, VPN, Cybersecurity and 5G validation solutions. Anand has 10+ years' experience in telecoms, working with digital and virtualization technologies and holds an MBA in technology strategy.***

# The Value of Independent Product Testing in Cybersecurity

Some practical steps to take when evaluating testing specifications, certifications, and products.

By Maxine Holt, Research Director, Omdia



At any one time there are around 4,000 vendors of cybersecurity products in the market – and even examining a comparable subset of these products can tee up a bewildering decision for a buyer. How does anyone know that Product A from Vendor A is better than Product B from Vendor B, when both products supposedly do the same thing?

Organizations have a range of options open to them. Analyst firms (Omdia included) publish comparative research reports, and these can be especially helpful in short-listing comparable products. Some organizations use a proof-of-concept (PoC) project as part of the decision-making process to see how the product performs in their environment.

A further option is to review certifications against open and independent testing specifications ("standards" is also used interchangeably and here means the same). There are typically three parties involved:

- **Party 1:** The independent body that creates a test standard/specification
- **Party 2:** The approved (and trusted) organization running the test against the specification
- **Party 3:** The vendor whose product is being tested

Independent testing against an open, industry-defined baseline specification helps buyers determine the capabilities of a product. This is nothing new – many readers will be familiar with independent "best buy" reports for consumers, covering everything from washing machines to televisions, flooring to roofing, and more besides.

Passing the test (run by **Party 2**) provides certification that the vendor (**Party 3**) can use to state that its product meets the minimum requirements as specified by the test specification (**Party 1**).

Such testing matters. Why? Because buyers can then compare apples with apples. But there are points to remember about these specifications and associated tests:

- Testing is about something specific. No single test checks the performance of everything in a product.
- Any test is a snapshot in time, relevant to the product, the environment, and the specification used for the test at that point.
- Tests are created by humans, and humans have interests. Open and independent testing specifications are designed to be exactly that – open to perusal and independent of influence – and should not be designed to show a product to its best advantage.
- The product tested should be one you can buy.
- Results have meaning – and limits. Whether the results are expressed in a single number or a spreadsheet full of data, the results say very specific things about the product being tested and the test being performed. The temptation can be great to draw far broader conclusions about the product than the test results can support.
- When you trust the specification and the test, trust the data. If you've vetted the test and trust both it and the organization that ran it, then you should trust the results. If they aren't what you expect, then there may be something you don't know about the product you're testing.

Here are some practical steps that organizations can consider when reviewing testing specifications, certifications, and vendor products:

- Know what the test is designed to measure and make sure it is measuring what you want to know about.
- If you're using a test designed by someone else, understand what their interests are and whether their interests align with yours. Independent specifications will avoid product bias.
- Make sure the product being tested is a real-world one with performance characteristics that you recognize.
- Make sure you know what the results can tell you, and on which subjects they are silent.
- Understand the limit of the results, no matter how they're expressed.

Remember that the objective of independent testing specifications and certifications is to provide openness and transparency to buyers, so that they can indeed compare apples with apples and see how different products compare to each other against the same test. Buyers may not always choose the best-performing product, but at least they will have a range of data and information to support their decision making.

**About the Author:** *Maxine leads Omdia's cybersecurity research, building and developing a comprehensive research program in this area to support vendor, service provider, and enterprise clients. Topics include infrastructure security, security operations, identity, authentication, and access, data security, IoT cybersecurity, and enterprise security management. Having worked with enterprises across multiple industries in the world of information security, Maxine has a strong understanding of enterprise security management – the Office of the CISO, the security challenges faced, and how organizations can look to overcome these challenges, with a particular interest in how all the component parts of security combine to make up an organization's security posture. LinkedIn: www.linkedin.com/in/maxineholt.*