No.4
11th April 2018

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

NetSecOPEN Faces St Augustine's Test

- Backed by several leading network security vendors, the new security testing group, NetSecOPEN, has just submitted an updated draft testing standard to the IETF.
- NetSecOPEN's members face their own version of St Augustine's dilemma when he asked to be "made chaste but not yet". If NetSecOPEN yields 'real world' test results that are lower than conventional testing benchmarks, will member vendors really be willing to leverage them in their sales and marketing campaigns?
- Buyers and vendors should actively embrace and support NetSecOPEN as its disruptive and transparent approach can enhance the network security ecosystem.

NetSecOPEN submitted an updated draft standard to the IETF for the testing of Next Generation Firewalls (NGFW) on March 22nd. The outcome is likely to be the publication in Q3 of an IETF RFC specifying a transparent testing methodology for these products.

"Buyers and vendors should actively embrace and support NetSecOPEN."

Supported by a number of the world's leading security vendors, NetSecOPEN is developing open standards for testing the capacity and security effectiveness of a variety of network security products. The goal is to drive more consensual, standards-based, test certification for buyers to evaluate security vendors. Specific use cases for the telecom sector are also planned.

NetSecOPEN: backdrop, membership and goals

NetSecOPEN is a non-profit, membership-driven organization, formed in 2017. Since test methodologies for NGFW are first up on NetSecOPEN's agenda, its first members are also leading lights among NGFW vendors.

Current vendor members are Check Point, F5, Fortinet, Palo Alto Networks, SonicWall and WatchGuard. Test equipment vendors IXIA and Spirent are also members, as are test labs EANTC, UNH-IOL and Underwriters Labs. Another thirty network security players are engaged and considering membership according to the organization.

Figure 1: NetSecOPEN's projected use-cases

Enterprises	Telcos
Enterprise FW	Business VPN service, Firewall, IDS & UTM
WAF	Mobile core & roaming firewall
Industrial & IoT FW	Protection of residential customers
NG IDS/IPS	Network management, perimeter firewall, IDS/IPS
Remote service VOIP FW	Application services, web portal firewall
UTM	

Source: NetSecOPEN

Its own mission statement states that NetSecOPEN is "a membership-driven network security industry group, created in response to the need for more insightful, realistic, up to date and non-proprietary evaluation and certification practices. NetSecOPEN standards will provide guidelines and best practices for testing modern network security infrastructure including Firewall, IPS, NGFW and threat detection solutions."

Through NetSecOPEN, security vendor members are looking to fill what they see as an important hole in the cyber security ecosystem (you could even think of it as a 'vulnerability'). This is that today there are no current testing methodology standards for testing security products that are recognized by any of the leading Standards Development Organizations (SDOs).

There is a ten-year-old RFC 3511 on the IETF's books relating to legacy firewall products. However, this doesn't take account of the key L7 capabilities that differentiates NGFW from legacy firewall products.

The current market in network security test certification

In the absence of industry-accepted standards, certification of security product performance in lab environments is led today by independent test houses such as NSS Labs and ICSA Labs. Their test methodologies are internally developed. While they do take account of vendor inputs, these current test methodologies don't appear as transparent as a consensus-driven model submitted to an SDO like the IETF according to NetSecOPEN's approach.

The current testing houses are extensively used by IT security vendors and buyers and they continue to exert considerable influence over vendor market share. However, the results they generate are often controversial, sometimes fiercely so. For example, CrowdStrike, FireEye and Palo Alto Networks have all engaged in very public spats with NSS Labs in recent years.

"A founding assumption is that the performance numbers generated by the current certification market take insufficient account of some real-world factors."

Founding assumptions of NetSecOPEN are that the performance numbers generated by the current certification market takes insufficient account of some key real-world factors and that greater transparency, consensus and standardization around testing methodology is needed. NetSecOPEN assumes that current test methodologies are yielding performance results that too often are unrealistically high, a sentiment that many enterprise buyers will recognize as well.

No-one wants to hear their baby's ugly

Most vendors certainly tend to care a lot less about the objectivity of test models when their own results leave competitors trailing in the dust than when they point to their own baby being ugly.

That makes the fact that all the major leading lights of the NGFW market are members of NetSecOPEN pretty impressive. It suggests that vendors themselves are craving more real-world, standards-based, test criteria to level the playing field and help develop the maturity of their own market place.

It also suggests a belief that they may be able to grow their own market share by outperforming competitors when certified against the new 'gold standard' in network security testing that NetSecOPEN wants to become.

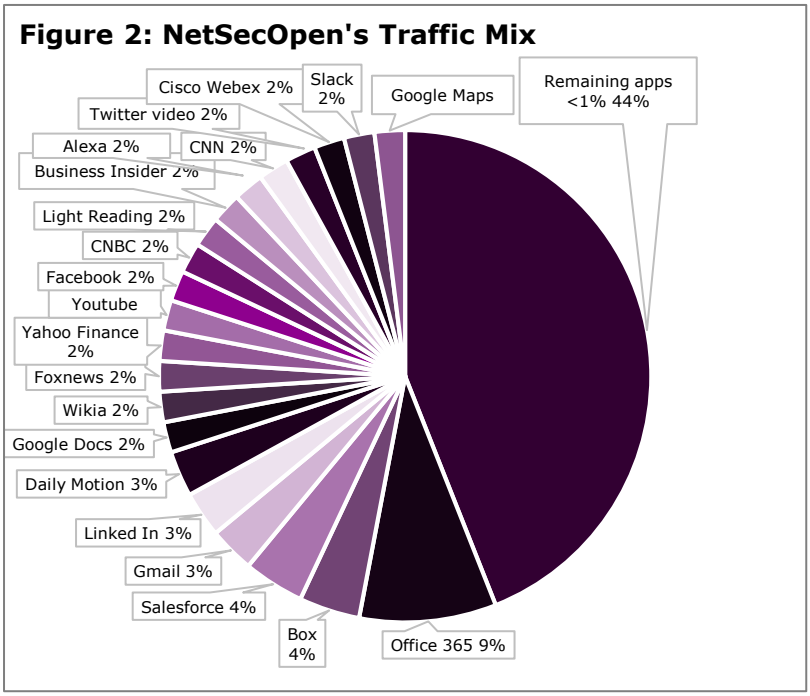
NetSecOPEN's approach to testing

There's an aspect of today's imperfect testing market that will always be with us. A vendor's relative performance compared with competitors is always likely to change in the context of a unique traffic mix. Hence the applicability to a specific environment of even the most objectively derived test results will always create at least some room for disagreement.

But there are aspects of the current market that NetSecOPEN believes it can clearly improve on. One relates to the way in which the test traffic mix is defined. NetSecOPEN is seeking to drive unprecedented, consensus-driven, insight into the criteria against which security products are tested by a NetSecOPEN-accredited test lab. The initial traffic mix for testing NGFW is shown in **Figure 2** on page 3.

Where vendors are accorded scores against an IETF security testing standard, the vision is that this will create a healthier ecosystem in network security products by providing more competition in the testing market; a more level playing field for suppliers; and ultimately enhanced credibility in the eyes of buyers.

Figure 2: NetSecOpen's Traffic Mix



Source: NetSecOPEN

As shown in **Figure 2** the traffic mix developed for NetSecOPEN has been developed by Spirent and has been approved by NetSecOPEN's members, including rival security test vendor, Ixia. According to NetSecOPEN, the traffic mix it has come up with has a number of key characteristics that render it a lot more relevant to a real-world networking environment.

Most notably the traffic mix includes 400 encryption certificates and 10,000 unique URLs. This is important because including these numbers in the test traffic mix chews up a lot of memory on the system resources of the products that are being tested.

NetSecOPEN recognizes this is likely to depress the number of concurrent sessions that tested security products are capable of supporting. The organization also recognizes that this will mean NetSecOPEN-certified results will probably come out lower against this key performance metric compared with conventional traffic mixes that tend to use fewer URLs and certificate numbers.

The IETF draft and the future roadmap

The first draft of testing standards relating to NGFW products was submitted to the IETF and discussed at the London IETF meeting on March 22nd. The security effectiveness requirements are due to be published late Q2 2018. Proof of Concept testing is due to begin shortly after, with the first round of certification testing scheduled for Q3 2018.

Next up on the priority list after NGFW products are testing standards for Next Gen Intrusion Protection Systems (NG IPS) and Web Application Firewalls (WAF). These are being targeted for IETF ratification during the first half of 2019. First standards development targeting the telecom sector as shown in **Figure 1** will also start in 2019.

NetSecOPEN members are also studying whether they should be turning their attention to security testing requirements for the IoT space.

The 'St Augustine Test' is still ahead

NetSecOPEN's members should be applauded for striving for more transparent standards in network security testing. In recent years the worlds of IT and telecom have seen large shifts in favour of greater openness, disaggregation and transparency.

It stands to reason that the same light should be shone into test methodologies and test certification. Buyers, as well as vendors in the supplier ecosystem, should therefore support NetSecOPEN. HardenStance is pleased to do so.

But while this is a critical moment, the specification of NetSecOPEN-driven standards by the IETF is no panacea. NetSecOPEN's biggest challenge still lies ahead. It was Saint Augustine who is said to have prayed "Lord, make me chaste (sexually pure) but not yet". Similarly, it's one thing for security vendors to embrace the ideal of more transparent, real-world, testing standards. It's another thing for them to actually use them front and centre in their day to day sales engagements, especially if the headline numbers don't look as good as those coming from other test houses.

Facing their own 'St Augustine Test', NetSecOpen's members will need to navigate a new model for using NetSecOPEN certification, including if the numbers that emerge are more "real-world". How exactly will Sales and Marketing VPs go about promoting those

more real-world outcomes? And when a competitor's product emerges as having a clearly better NetSecOPEN test score, how will those VPs spin that?

The whole point of NetSecOPEN is to take the "No way! We were cheated!" option off the table. Then again, "fair play, we're grateful to NetSecOPEN for demonstrating beyond any doubt that our product really is inferior" won't ever make it onto the table either.

Vendors' technical teams seem to have been playing together very nicely in bringing the first NetSecOPEN efforts so close to standardization. The baton is now set to pass to their commercial counterparts to keep this excellent momentum going.

That won't be easy. The alignment in the agendas of the VP, Sales and his or her guy that runs sales in Egypt, the Nordics or the Dakotas is often less than perfect. Getting the sales folks on the ground on-side is going to be every bit as important.

Buyers have a critical role to play too. If they like what NetSecOPEN stands for, they need to be vocal in driving demand for it ■

For more information about HardenStance, visit **www.hardenstance.com**

For more information about NetSecOPEN, visit **www.netsecopen.org**

- HardenStance received no payment – direct or "in kind" – for publishing this Briefing.
- **Contact HardenStance's Principal Analyst:** patrick.donegan@hardenstance.com
- **Register here** for **free email notifications** whenever new IT and telecom security content is made available by HardenStance.
- In response to HardenStance's request to discuss NetSecOPEN and its potential impact on the market, NSS Labs emailed the link to its **FAQ: NSS Labs Mission and Tests** page.
- **See Disclaimer on the last page**

HardenStance Ltd Disclaimer of Warranty and Liability

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.