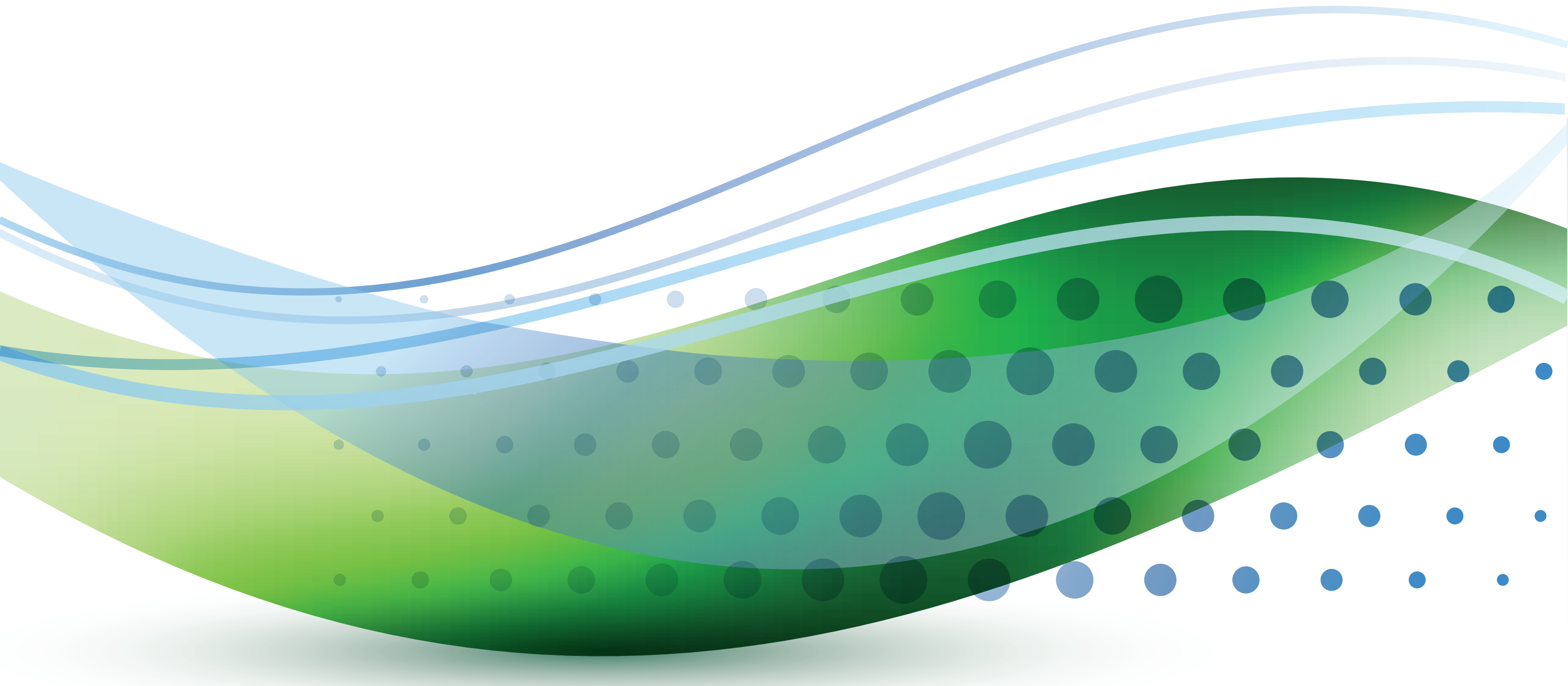
EANTC

EANTC Independent Test Report

Accreditation Report: Viavi TeraVM

NetSecOPEN Test Methodology

May 2020



NetSecOPEN

Authorised Test Tool

VIAVI

Introduction

EANTC has been commissioned by Viavi to accredit the Viavi TeraVM test solution for use with the NetSecOPEN test methodology. Viavi has passed our accreditation tests and has successfully been accredited by NetSecOPEN.

The accreditation and this report cover the ability of Viavi's TeraVM to test Next-generation firewalls (NGFW) – advanced network security solutions. A NGFW is expected to protect reliably from a wide range of threats. Its effectiveness must be evaluated by adequate throughput performance and session scale scenarios while testing advanced threat protection realistically at the same time.

Until today, it has been very hard to access independent, reliable and reproducible performance data of next-gen firewalls. Datasheets are published using different approaches, are not comparable and represent maximum numbers achieved in the lab. Only a small number of enterprises worldwide have the knowledge, time and funding to evaluate and compare firewall performance realistically themselves. Most enterprises follow analyst ratings. Analysts, in turn, usually get their information from the manufacturers' data sheets. Actual public testing has been rare so far, has often not been sufficiently realistic, could not be compared across test houses, and is in danger of vendor influence - as the details of test methodology are not usually published, making independent verification impossible.

To solve these issues, NetSecOPEN was founded by test tool manufacturers, multiple test labs, and multiple firewall vendors in 2018. EANTC joined NetSecOPEN as a founding member. Our goal at EANTC matches the NetSecOPEN goals: To evolve network security product evaluation and to provide reliable, reproducible firewall benchmarks freely available to enterprises. At EANTC, all our test methods are public, fully transparent and prepared under the supervision of the Internet Engineering Task Force (IETF). After two years of preparation, NetSecOPEN and EANTC have kicked off certification testing in February 2020.

Viavi TeraVM is joining the group of test tool vendors implementing the NetSecOPEN methodology. EANTC, as a NetSecOPEN-accredited test lab, has conducted extensive tests to verify the compliance of Viavi's implementation with NetSecOPEN requirements, in coordination with the NetSecOPEN Certification Authority (CA). These requirements are based on an IETF draft standard[1] co-authored by EANTC.

Test Highlights

- → TeraVM supports the NetSecOPEN parameters and KPIs
- → 380,000 HTTP Connections Per Second and average TTLB of 1.7 ms with 1 KB object size
- → 11.84 Gbps HTTP Throughput and average TTLB of 3.2 ms with Mixed object size
- → 500,000 Concurrent HTTP Connections and average TTLB of 0.36 ms with 1 KB object size
- → 1.17 ms as average TTFB for 50% of maximum HTTP Throughput with 256 KB object size
- → 0.693 ms as average TTLB for 50% of maximum HTTP Throughput with 1 KB object size
- → 1.221 ms as average TTFB for 50% of maximum HTTP CPS with 2 KB object size
- → 1.312 ms as average TTLB for 50% of maximum HTTP CPS with 1 KB object size
- → 3,000 HTTPS Connections Per Second with 2 KB object size
- → 8.06 Gbps HTTPS Throughput with 256 KB object size
- → 250,000 Concurrent HTTPS Connections with 1 KB object size
- → 3.81 ms as average TTFB for 50% of maximum HTTPS Throughput with 1KB object size
- → 1.10 ms as average TTLB for 50% of maximum HTTPS Throughput with 1 KB object size
- → 3.43 ms as average TTFB for 50% of maximum HTTPS CPS with 4 KB object size
- → 3.43 ms as average TTLB for 50% of maximum HTTPS CPS with 4 KB object size

[1] https://tools.ietf.org/html/draft-ietf-bmwg-ngfw-performance-02

TeraVM is a fully virtualized test solution. Viavi brought an integrated solution to EANTC's test, running on a Dell R630 server with four 10 GigabitEthernet interfaces. All tests were conducted between October 2019 and January 2020.

Executive Summary

EANTC verified that the Viavi TeraVM traffic generator and protocol emulator supports all the protocols and cipher suites required by NetSecOPEN. It is able to conduct all test cases in accordance with the current IETF draft: The next-generation firewall throughput and latency benchmark, the connections per second test, and the maximum number of concurrent connections tests both for unencrypted HTTP and encrypted HTTPS scenarios. In parallel, TeraVM can generate a selected number of emulated threats to verify a firewall's ability to protect against attacks.

Since TeraVM is a virtualized solution, EANTC focused the evaluation of the benchmarking tests within the limits of the specific hardware provided by Viavi for this test. For us, it was most important that the data plane traffic flows, test management and control as well as statistics of TeraVM are implemented correctly. We verified that the TeraVM was able to meet all of our expectations with regards to the functional correctness and benchmarking methods in principle. The absolute performance was not the main goal of EANTC's evaluation. NetSecOPEN accreditation does not mandate any specific absolute performance requirements.

Software Details

Components	Software Version
TeraVM Executive VM (TVM-E)	TeraVM v14.5
TeraVM Controller VM (TVM-C)	TeraVM v14.5
TeraVM Test Module VM (TVM-5)	TeraVM v14.5
Hypervisor	VMware ESXi 5.5

Table 1: Software Versions

Testbed Description

Viavi TeraVM solution is a virtualized solution which provides application emulation and security performance services. The main components of the solution are TeraVM Executive VM, TeraVM Controller VM, and TeraVM Test Module VM. TeraVM Executive VM (TVM-E) provides a number of centralized services in a TeraVM test environment. These services include a shareable Centralized Test Library, User Authentication settings, Pool Manager, DHCP management, and License Tracker. Meanwhile, the TeraVM Controller VM (TVM-C) sets up a TeraVM test, directs TeraVM Test Module VM's to generate and receive IP traffic, executes the test and processes results. The TeraVM Test Module VM (TVM-5) generates and receives IP traffic. Each of TVM-5 is connected to a physical port via Direct Path Configuration.

In the test, TeraVM solution was on-boarded on a Dell PowerEdge R630 server with two Intel 10 GbE Dual-Port NICs, 36 CPU cores and 256 GB RAM. The TeraVM solution was configured with the following resources.

TeraVM solution was configured with the following resources.

- TVM-E: 2x vCPUs and 4 GB memory
- TVM-C: 1x vCPUs and 4 GB memory
- TVM-5: 5x vCPUs and 10 GB memory

TeraVM Back-to-Back Setup

As shown in Figure 1 each of the 4x TVM-5 is connected to a 10 GigabitEthernet interface via ESXi direct path configuration. We used two interfaces for client side and another two interfaces for server side. Since the test is focused on a back to back test, we connected the relative client and server ports as back-to-back.

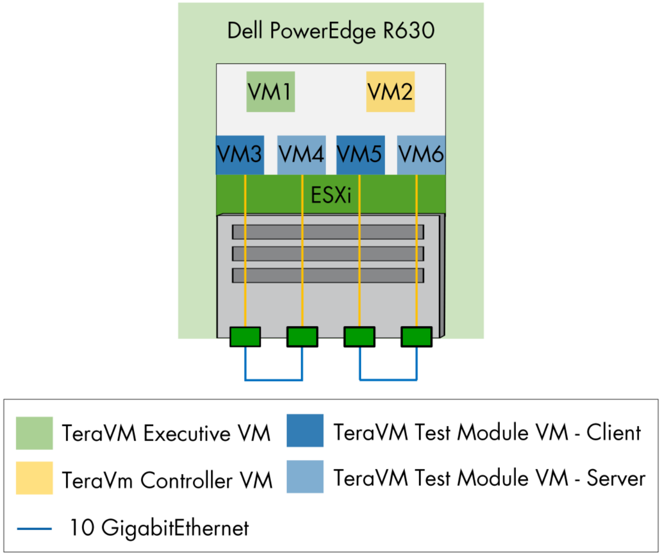


Figure 1: Logical Topology for Back-to-Back Test

TeraVM against virtual Firewall Setup

For this setup, we connected the two 10 GigabitEthernet physical interfaces of TeraVM solution to the two Gigabit Ethernet physical interfaces of a virtual firewall solution via a physical switch as in Figure 2.

The below screenshot depicts the Viavi TeraVM's web based Graphical User Interface (GUI). The web GUI is used to configure the traffic flows and observe the traffic statistics of the current traffic flows.

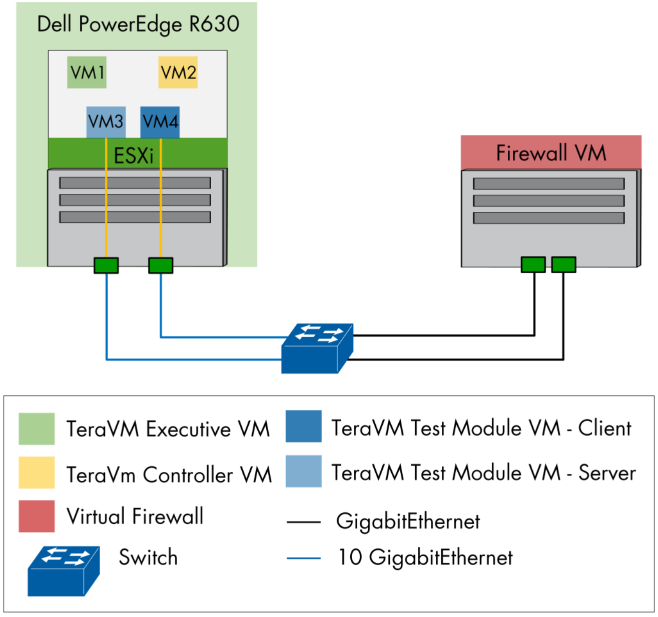
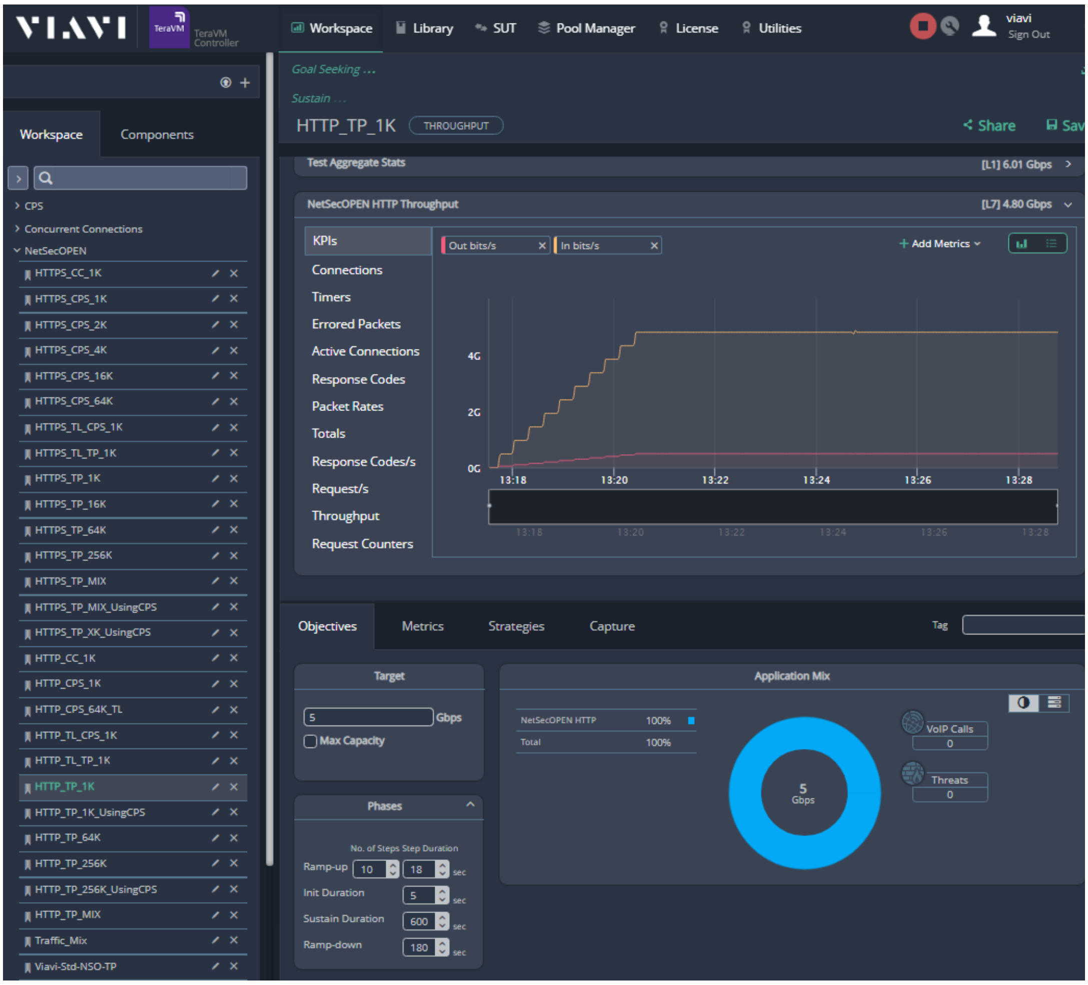


Figure 2: Logical Topology for TeraVM Test Environment and virtual Firewall



[L1] 6.01 Gbps

[L7] 4.80 Gbps

Target: 5 Gbps

□ Max Capacity

	No. of Steps	Step Duration	
Ramp-up	10	18	sec
Init Duration		5	sec
Sustain Duration		600	sec
Ramp-down		180	sec

NetSecOPEN HTTP	100%	🟦
Total	100%	

VoIP Calls: 0

Threats: 0

Figure 3: TeraVM GUI

Traffic Generator Parameters

For this test, the TeraVM solution was configured with the recommended NetSecOPEN parameter list as below.

Parameter	Value
TCP (for client and server)	
TCP windows size	65535
MSS	1460
Congestion window	14600
No. of Re-transmission	3
Delayed ACK	All segments ACK for HTTP tests, 2 segments timer based ACK for HTTPS tests
Three-way handshake	Yes
HTTP/HTTPS Browser	
HTTP version	1.1
Persistence connection	Yes
Advertise user-agent header	Yes
Uncompressed data	Yes
Validate content length	Yes
Support X transaction per connection	Yes
Think time/waiting time between two transactions	Yes
For encrypted traffic	
Support TLS 1.2 or more	Yes
Send TLS Extension Server Name Indication (SNI) information	Yes
No Session reuse/resumption	Yes
Record size	16383
Support ciphers and key defined in the draft	Yes
HTTPS Server	
Record size	16383
Host SNI with FQDN	Feature is configurable, but, not used for the current test
Cipher suit and keys are configurable as defined in the draft	Yes Cipher used for this test - ECDHE RSA AES128 GCM SHA256 with RSA 2048 Signature Hash Algorithm: rsa_pkcs1_sha256 and Supported group: sepc256
IP (client and server)	
Support number of IPs and subnets	Yes, number of IPs are configurable both client and server side
ToS value	Yes
IPv6 support	Yes
Traffic Profile	
Support all 4 phases as defined in the draft	Yes (Init, Ramp-up, Sustain, Ramp-down)
Reporting	
Results polling frequency 2-5 seconds	Every 1 second

Table 2: Parameter for Tester Configuration

Test Results

We performed the eight test cases which are defined in the NetSecOPEN standards with different object sizes. The test validates that the defined NetSecOPEN parameters and KPIs can be configured and measured by the TeraVM solution. Our tests included both unencrypted and encrypted web traffic (HTTP and HTTPS protocols). We conducted separate tests for each metric below:

- Throughput
- Connections per seconds
- Maximum number of concurrent connections
- Transaction latency

These tests were performed for HTTP and HTTPS traffic separately with IPv4 and TCP traffic. As in the test bed description, we executed the test with back-to-back setup first and then performed one more test with the firewall setup. This report interprets the back-to-back test results only.

In the test against a virtual NGFW, this firewall was enabled with antivirus detection, application control, and Secure Socket Layer (SSL) inspection as per NetSecOPEN standard requirement. Using the firewall setup, we confirmed that the TeraVM solution measured the required KPIs with the enabled mandatory features of the firewall solution. The NGFW identity is not disclosed in this report; that said, EANTC has verified that the NGFW met the criteria for NetSecOPEN certification and was a suitable object for TeraVM accreditation.

HTTP Throughput

This test ensures the maximum throughput performance supported by Viavi TeraVM solution with the current setup as mentioned in the testbed description above. As per the test methodology defined in NetSecOPEN, the TCP sessions are kept open longer, using each session for 10 consecutive HTTP transactions.

For each test run, TeraVM was configured to run the test for 960 seconds with 180 s ramp up time, 600 s sustain phase, and 180 s ramp down time. During the sustain phase, we measured the maximum throughput and maximum Transactions Per Second (TPS) for each object size recommended by NetSecOPEN.

The results shows that TeraVM can be expected to generate IPv4 unencrypted HTTP traffic in about the 11-Gigabits-per-second range for the object sizes from 16 KB to 256 KB and for Mixed object size. The throughput figures were achieved with a latency of 3.8 ms. As expected, the total throughput is much lower for small 1 KB object size. The device reaches 5.21 Gbit/s.

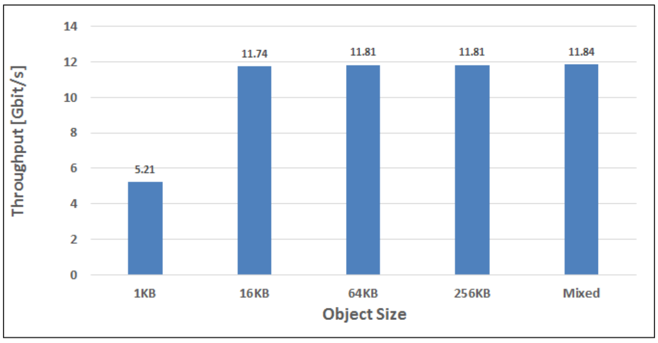


Figure 4: HTTP Throughput Results

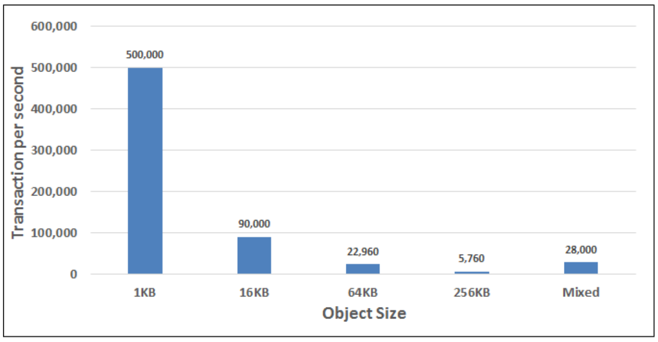


Figure 5: HTTP Throughput Results – TPS

This result shows that the overhead of setting up a new TCP session is quite high. Since the throughput test utilizes each single TCP session for ten HTTP transactions, 500,000 transactions relate to 50,000 TCP sessions per second. There were no transaction failures or TCP errors during the test.

HTTPS Throughput

We conducted a pure HTTPS throughput test with the exact same configuration as the (unencrypted HTTP) test case above. The only difference was that we setup TCP/SSL sessions, each servicing ten (10) transactions as before. The cipher mentioned in Table 2 was used for the test.

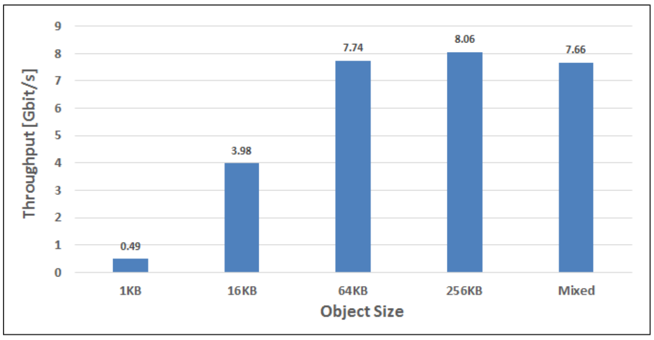


Figure 6: HTTPS Throughput Result

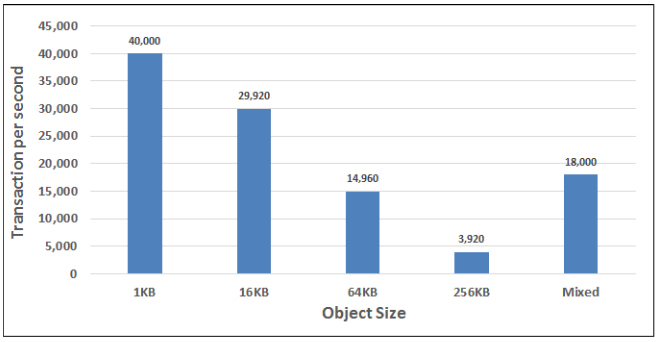


Figure 7: HTTPS Throughput result – TPS

TeraVM reached the maximum throughput as 8.06 Gbit/s for 256 KB object size with the encrypted traffic. The observed latency was 24 ms. Figure 6 clearly shows that the larger the object size, the higher throughput results are achieved. For the small 1 Kilobyte object size, the additional overhead of setting up the encrypted session is reflected in the overall lower throughput numbers. Comparing with the throughput values, the number of transactions per second shows the inversely proportional relationship with the object sizes. The smallest object sizes come with the highest rate of transaction.

TCP/HTTP Connections Per Second (CPS)

The purpose of the test is to measure the maximum accepted new TCP connection establishment rate supported by the TeraVM solution under different object sizes recommended by NetSecOPEN. Meanwhile this test also verifies that the mandatory KPIs of the test can be measured by the TeraVM solution. As per the test methodology, we configured the TeraVM test tool to use one single HTTP transaction per TCP session. Once the HTTP transaction had been successfully completed, the test tool closed the TCP session immediately as expected, using the three way handshake of TCP FIN. For each test run, TeraVM was configured to run the test for 960 seconds with 180 s ramp up time, 600 s sustain phase, and 180 s ramp down time. We measured the average TCP connection per second for each object size during the sustain phase.

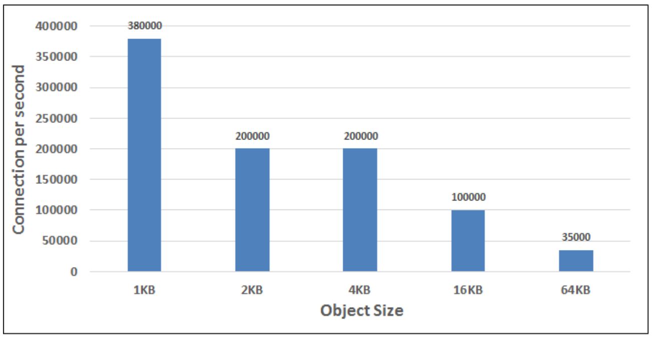


Figure 8: HTTP Connections Per Second

The results show a maximum number of 380,000 connections per second at the smallest object size of one Kilobyte. The results related to larger object sizes are lower, as expected. We noted that there were no transaction failures or TCP errors during the test.

TCP/HTTPS Connections Per Second

We repeated the CPS test again with the encrypted connections which means each TCP sessions are established with SSL. The remaining parameters were same as in the previous CPS test.

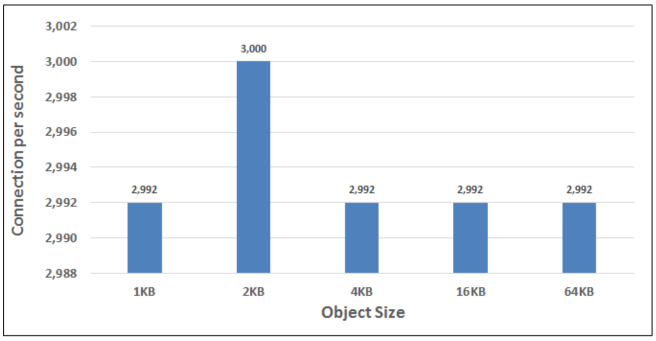


Figure 9: HTTPS Connections Per Second

As shown in Figure 9, we measured 2,992 connection per seconds for the object sizes 1 KB, 4 KB, 16 KB, and 64 KB. The CPS for 2 KB was the highest value than the other object sizes. According to Viavi solutions, the CPS rate measured can have small deviations in each sampling interval.

Concurrent Connection Capacity

In the test, we determined the maximum number of simultaneously open connections that the TeraVM solution can generate when using HTTP traffic. We performed this test following the generic methodology of the throughput test: Conducting ten HTTP (or HTTPS) transactions per TCP (or TLS) session. After the ten transactions had been completed, we closed the session as in the throughput test. The difference in this test case was that we inserted 90 seconds of so-called "think time" after each transaction so that the session could remain established long enough during the whole sustain phase. During the ramp-down phase, we verified that all sessions were closed correctly, reconfirming that the sessions had remained active throughout the steady phase. The test contains 180 s ramp-up time, 720 s sustain phase and 180 s ramp-down time.

TeraVM generated 500,000 concurrent HTTP connections in the unencrypted scenario. In a separate test run with encrypted sessions only, the TeraVM managed to maintain 250,000 concurrent HTTPS connections. We did not observe any unexpected behavior during these test runs.

HTTP Transaction Latency

The purpose of the test is to determine the average HTTP transaction latency when TeraVM solution is running with sustainable HTTP transactions per second supported by the TeraVM solution under different HTTP response object sizes. As per the NetSecOPEN, the Time To First Byte (TTFB) is measured from the time of TCP session creation (syn packet) until the first packet received by the client. Meanwhile, the Time To Last Byte (TTLB) is measured from the first get request of client until the last packet of the transaction received by the client. As defined in NetSecOPEN, the transaction latency test must be measured in two different scenarios. One with a single transaction as CPS test and the other with multiple transactions within a single TCP connection as tested in the throughput test. We performed the test two times, (1) with 50% of the maximum CPS measured in test scenario TCP/HTTP Connections Per Second, and (2) 50% of the maximum throughput measured in test scenario HTTP Throughput. The objects used were same as in the CPS and the throughput test. TeraVM was configured to run the test for 960 seconds with 180 s ramp up time, 600 s sustain phase, and 180 s ramp down time. We measured the minimum, average, and maximum value of TTFB and TTLB for each object size during the sustain phase.

The following Figures illustrate the TTFB and TTLB behavior for the 50% of maximum HTTP throughput test.

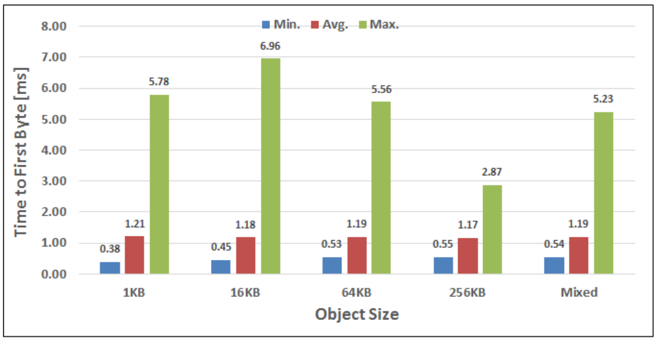


Figure 10: HTTP Transaction Latency with 50% of Maximum HTTP Throughput – TTFB

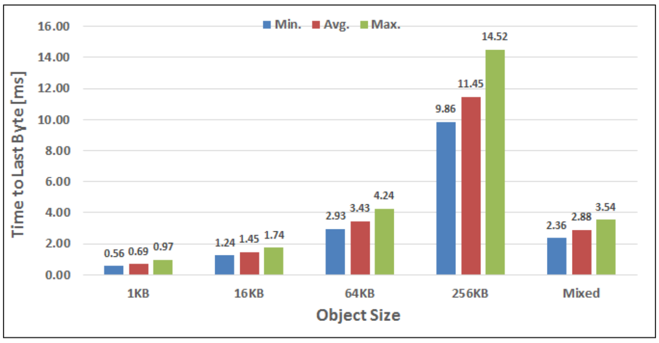


Figure 11: HTTP Transaction Latency with 50% of Maximum HTTP Throughput – TTLB

Figure 10 shows that the lowest maximum TTFB was measured at 256 KB object size with the value of 2.87 ms. Since the packet processing for large object size is lower than small object size, the TTFB for large object size has low value.

The maximum TTFB value was observed for 16 KB with the value of 6.96 ms. According to Viavi solutions, the TTFB measured can have small deviations in each sampling interval.

As expected, the TTLB for large object size is higher since the complete transaction takes time for the large object size. We observed 14.52 ms as the maximum TTLB for 256 KB.

The Figures below show the TTFB and TTLB behavior for the 50% of maximum HTTP CPS test.

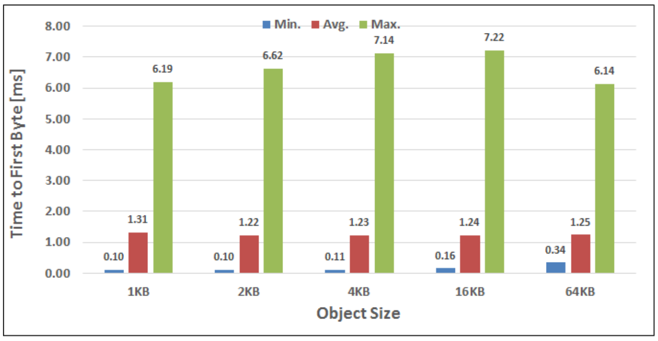


Figure 12: HTTP Transaction Latency with 50% of Maximum CPS – TTFB

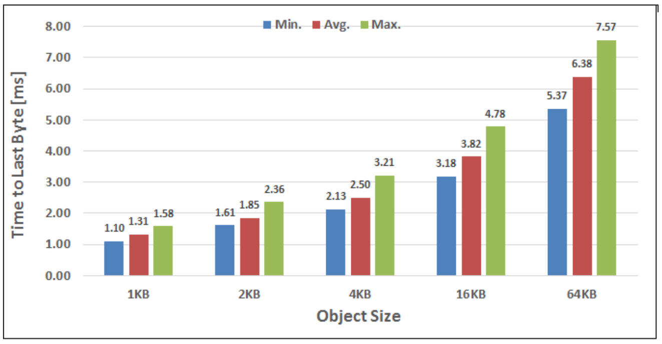


Figure 13: HTTP Transaction Latency with 50% of Maximum CPS – TTLB

As shown in Figure 12, the maximum TTFB values for different object sizes are nearly identical in the range of 6.1 ms to 7.2 ms. The maximum TTFB value, 7.22 ms, was measured with a 16 KB object size. As expected, the TTLB values increase with the increasing object sizes.

HTTPS Transaction Latency

We repeated the transaction latency test with the encrypted connections which means each TCP session was established with SSL. The remaining parameters were same as in the previous HTTP Transaction Latency test. We measured the minimum, average, and maximum value of TTFB and TTLB for each object size during the sustain phase.

The following Figures illustrate the TTFB and TTLB behavior for the 50% of maximum HTTPS throughput test.

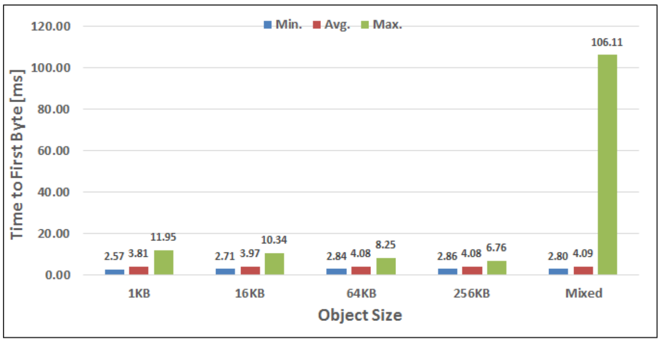


Figure 14: HTTPS Transaction Latency with 50% of Maximum HTTPS Throughput – TTFB

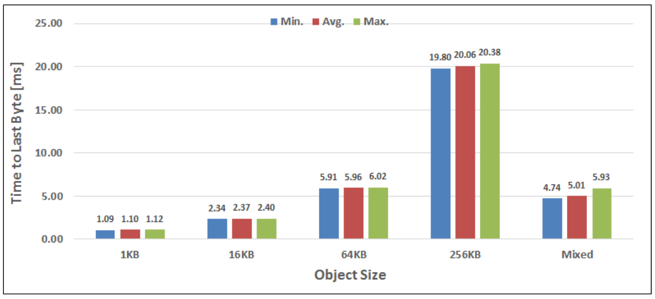


Figure 15: HTTPS Transaction Latency with 50% of Maximum HTTPS Throughput – TTLB

As expected, the lowest TTFB value was observed at 256 KB with the value of 6.76 ms. For the Mixed object size, we observed a highest TTFB which is a one time maximum value.

As shown in Figure 15, the highest object size has the highest TTLB value and the lowest packet size has the lowest value of TTLB.

The Figures below shows the TTFB and TTLB behavior for the 50% of maximum HTTP CPS test.

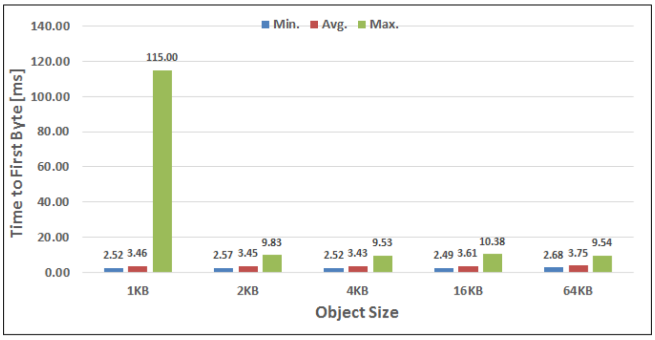


Figure 16: HTTPS Transaction Latency with 50% of Maximum CPS – TTFB

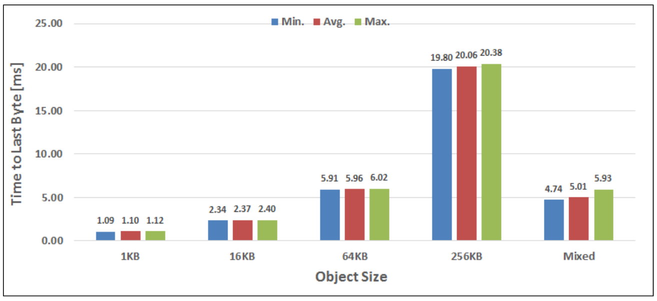


Figure 17: HTTPS Transaction Latency with 50% of Maximum CPS – TTLB

The maximum TTFB for the object sizes 2 KB, 4 KB, 16 KB, and 64 KB are in the range of 9.5 ms to 10.3 ms.

We observed an unexpected highest TTFB with 1 KB object size. This was a one time maximum value.

As expected, the TTLB values increase with the increasing object sizes except 1 KB object size.

Conclusion

We tested the TeraVM solution in two aspects. In the first aspect, we confirmed that the TeraVM solution is capable to configure the NetSecOPEN test parameters and it can also produce the mandatory KPI results for the NetSecOPEN tests. In the second aspect, we verified the maximum performance of the TeraVM solution when we use current setup for the back-to-back test.

During the back-to-back performance test, TeraVM showed solid performance and stable operations. We verified the maximum throughput as 11.84 Gbit/s for unencrypted traffic with Mixed object size and average TTFB of 1.321 ms. For encrypted traffic, we measured 8.06 Gbit/s with 256 KB object size and average TTFB of 4.356 ms. TeraVM solution could also generate 380,000 unencrypted HTTP connections and 3,000 encrypted HTTPS connections per second with 1 KB object size. We measured 500,000 concurrent connections for HTTP and 250,000 concurrent connections for HTTPS. Finally, we measured the HTTP and HTTPS transaction latency with the parameters TTFB and TTLB. The average TTFB was measured as 1.7 ms / 3.81 ms at 256 KB / 1 KB for HTTP/HTTPS throughput traffic profile. For the same HTTP/HTTPS throughput traffic profile, we measured the average TTLB as 0.69 ms / 1.10 ms at 1 KB. Meanwhile, we measured TTFB and TTLB for HTTP and HTTPS CPS traffic profiles. The average TTFB was measured as 1.221 ms / 3.43 ms at 2 KB / 4 KB for HTTP/HTTPS CPS traffic profile. The average TTLB value for the HTTP and HTTPS CPS was 1.31 ms at 1 KB and 3.43 ms at 4 KB object size.

We conducted all tests on a specific virtualization platform supplied by Viavi for this test. Generally, performance aspects of virtualized tools such as maximum throughput, minimum latency or session scalability depend on the underlying hardware scale, software platform configuration and the desired traffic workload. Viavi confirmed that they will provide guidelines for measuring the baseline performance of the virtualization layer for NetSecOPEN testing with the above variables.

EANTC confirms that Viavi TeraVM can be used to successfully execute NetSecOPEN certification test cases 7.2 through 7.9 (full certification scope as of May 2020).

Once NetSecOPEN will have defined the procedures on how to run and measure firewall detection efficacy, Viavi will run the related Common Vulnerabilities and Exposures (CVE®) tests.

About EANTC

EANTC (European Advanced Networking Test Center) is internationally recognized as one of the world's leading independent test centers for telecommunication technologies. Based in Berlin, the company offers vendor-neutral consultancy and realistic, reproducible high-quality testing services since 1991. Customers include leading network equipment manufacturers, tier 1 service providers, large enterprises and governments worldwide. EANTC's Proof of Concept, acceptance tests and network audits cover established and next-generation fixed and mobile network technologies.

While every reasonable effort has been made to ensure accuracy and completeness of this publication, the authors assume no responsibility for the use of any information contained herein. All brand names and logos mentioned here are registered trademarks of their respective companies in the United States and other countries.

EANTC AG
Salzufer 14, 10587 Berlin, Germany
info@eantc.de, http://www.eantc.de/
[v1.0 20200525]