EANTC Lab Report
NetSecOPEN Certification Test
Fortinet FortiGate 500E

Version 1.1
2020-02-11

EANTC AG

1. Date and time of the test

2020-Jan-04, Berlin, Germany

2. Summary of the testbed software and hardware details

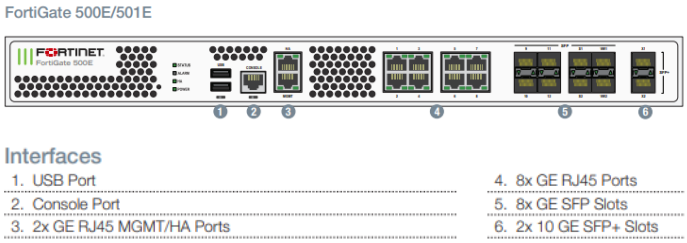


Figure 1: Port Interfaces, with speed and link info

DUT Hardware	Next-Generation Firewall
Brand and model	Fortinet FortiGate 500E
Any additional hardware used by the DUT	2x FINISAR FTLF8519P3BNL 1GE SFP 2x HPX130 10G SFP+

Table 1: Testbed Details

3. DUT Software

Note: DUT config used must be provided to NetSecOPEN certification body.

```
EANTC-FGT_500E # get system status
Version: FortiGate-500E v6.0.6,build0272,190716 (GA)
Virus-DB: 73.00168(2019-11-18 14:19)
Extended DB: 73.00168(2019-11-18 14:19)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 14.00725(2019-11-15 02:08)
APP-DB: 14.00725(2019-11-15 02:08)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
Serial-Number: FG5H0E5819902236
IPS Malicious URL Database: 2.00468(2019-11-18 08:07)
Botnet DB: 4.00613(2019-11-12 19:19)
BIOS version: 05000005
System Part-Number: P21591-05
Log hard disk: Not available
Hostname: EANTC-FGT_500E
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 3 in NAT mode, 0 in TP mode
Virtual domain configuration: enable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 0272
Release Version Information: GA
FortiOS x86-64: Yes
System time: Fri Dec 13 18:26:15 2019
```

Figure 2: Operating System

Version	6.0.6

Table 2: DUT Software

Figure 3: Specific configuration

4. Test Equipment

Test equipment vendor name	Spirent
Hardware details - including model and interface type	
Model	C100-S3
Interface type	8x 10GE SFP+, 8x 1GE RJ45
Firmware and test application software version	
Chassis OS	5.03.0389
Avalanche Commander	5.03 build 1196 32bit
Cyberflood controller	19.4.0.3105
HPE 5900AF-48XG-4QSFP+ Switch	7.1.045, Release 2422P01

Table 3: Test Equipment Details

Note: Spirent TCP CRC hardware offloading is disabled, Spirent pseudo test FPGA fill is disabled.

Changes made to the default test tool configurations - Disabled the goal seeking mode. We set up the load based on the target throughput disclosed by Fortinet. We also changed the ramp-up, sustain phase, and ramp-down time.

5. Name and version of the draft standard

Benchmarking Methodology for Network Security Device Performance (draft-ietf-bmwg-ngfw-performance-02)

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

6. Executive Summary

The Fortinet FortiGate 500E participated in the NetSecOPEN certification scheme for next-generation firewalls (Q1/2020 release). The solution passed all eight test areas. There were no unexpected situations encountered. Fortinet supported the tests and provided the latest software version of Forti OS, 6.0.6, for optimal results.

Specifically, the FortiGate 500E performed well in the HTTP and the HTTPS test cases. It showed throughput of more than 6.4 Gbit/s for cleartext HTTP connections, and more than 5.4 Gbit/s in a pure HTTPS encrypted scenario. The tests were carried out with large uniform object sizes of 256 Kilobytes each, and with an up-to-date cipher in the encrypted case. The throughput achieved with smaller object sizes is lower as expected, and documented in this report as well (see below).

In separate test cases, the FortiGate 500E managed up to 1.55 Million simultaneous unencrypted HTTP connections, or alternatively roughly half of this number (745,000) encrypted HTTPS connections. Session scale is important to ensure that the firewall can keep all sessions in mind, even if there are a large number of low-bandwidth, long-lived sessions.

Finally, we measured the session setup speed - which is important to ensure agile operations with fast user response in typical web access situations. In such cases, a large number of short-lived sessions are established. The FortiGate 500E managed to setup more than 22,400 unencrypted HTTP connections per second. Alternatively, it can handle up to 3,103 new HTTPS sessions per second. The difference is expected because setting up HTTPS connections involves more messages per each session.

All tests were carried out in the presence of active threats - to ensure that the firewall is able to protect from attacks at all conditions and loads. The threat protection worked correctly in all situations we evaluated.

Tests were performed by enabling Logging and Reporting features of the DUT.

EANTC confirms that the performance of the FortiGate 500E is well suited for mid-sized enterprise perimeters and comparable scenarios, requiring the throughput performance and session scales witnessed, while providing adequate protection from a wide range of threats.

7. Test Setup

7.1. Testbed Configuration

Initially, we used Figure 2 in section 4.1 from the draft with virtual routers enabled in the beginning. However, Spirent Cyberflood didn't support virtual router in the CVE test case. Therefore, Fortinet created one additional vdom that contained identical configuration as mainly test vdom. As there are only two 10 GbE interfaces on Fortinet, we used a switch in the middle to convert the link speed from 10 G to 1 G. The final testbed used for the tests is given below. It is a mix of Figure 1 and 2 in section 4.1 from the draft.

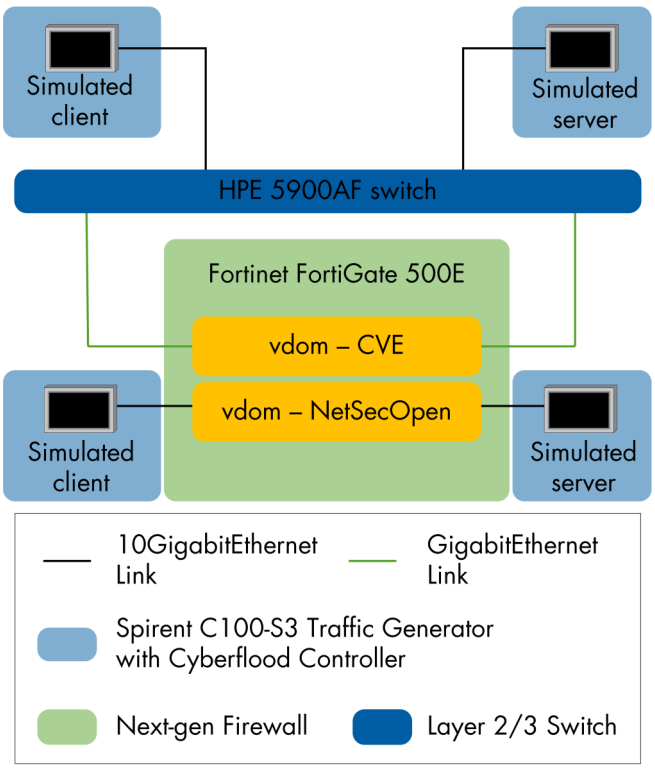


Figure 4: Testbed Setup

7.2. DUT/SUT Configuration

DUT features	Mapped requirement in the draft
Antivirus	Antivirus Anti-Spyware
Application Control	Application Identification
IPS	IDS/IPS Anti-Botnet
SSL inspection	SSL inspection
Log	Logging and reporting

Table 4: DUT/SUT feature list

Note: Logging and reporting were enabled. However, as the 500E doesn't contain a hard disk, all the log info had been forwarded to an external host.

From the 500E datasheet, we see its NGFW throughput is 5 Gbps. Therefore, we chose the S profile from the draft for Fortinet to configure. More details are in the configuration guide documentation.

We did a spot check for the policies. It blocked all the traffic based on our configuration guide. The details are in the result.

The virtual router function of the Spirent Avalanche was enabled. This way, the FortiGate 500E received all traffic via only one MAC address per port. The traffic was isolated by switch Virtual Routing and Forwarding (VRF).

8. Test Results

8.1. TCP/HTTP Connections Per Second

We executed this test with Spirent automation script v1.6. The test contained 180 s ramp-up time, 600 s sustain phase and 180 s ramp-down time. All the test results met the requirements of "7.2.3.3. Test Results Validation Criteria" except item d. The CC deviation was more than 10%. However, the trend of the deviation tended to be stable instead of increasing. Therefore, we evaluated the test result to meet the item d.

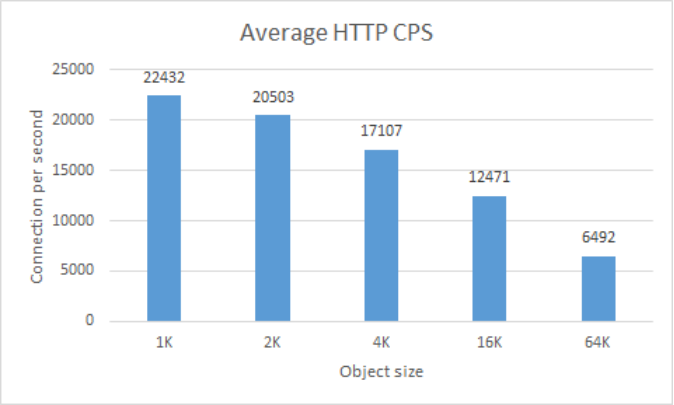


Figure 5: HTTP CPS Result Summary

8.2. HTTP Throughput

We executed this test with Spirent automation script v1.6. The test contained 180 s ramp-up time, 600 s sustain phase and 180 s ramp-down time. All the test results met the requirements of "7.3.3.3. Test Results Validation Criteria" except item c. The CC deviation was more than 10%. However, the trend of the deviation tended to be stable instead of increasing. Therefore, we evaluated the test result to meet the item c.

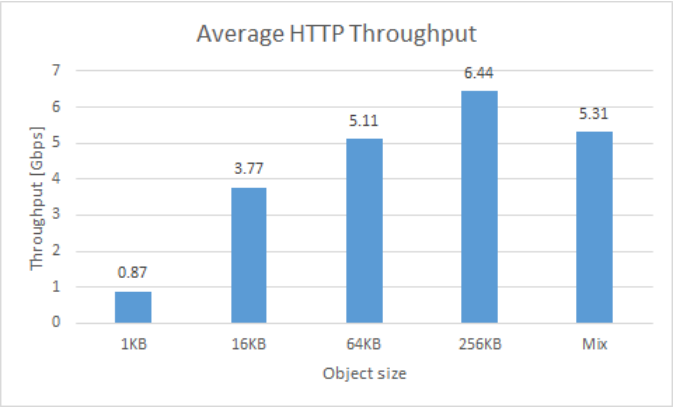


Figure 6: HTTP Throughput Result Summary

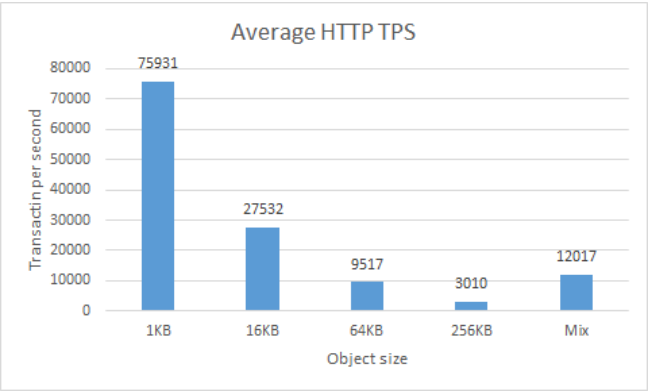


Figure 7: HTTP Throughput Result Summary

8.3. TCP/HTTP Transaction Latency

We executed this test with the Spirent automation script v1.6. The test contained 180 s ramp-up time, 600 s sustain phase and 180 s ramp-down time. All the test results met the requirements of "7.4.3.3. Test Results Validation Criteria".

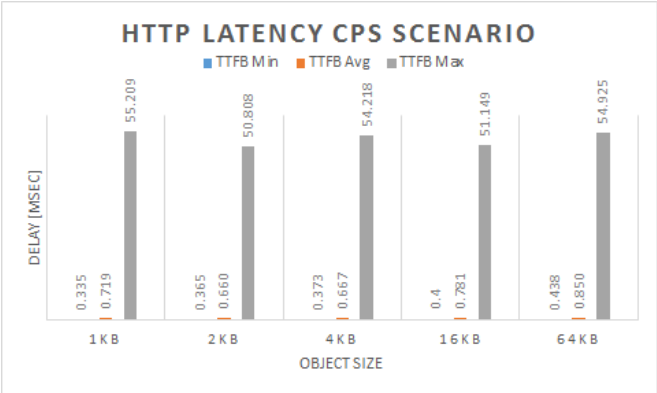


Figure 8: HTTP Transaction Latency Result Summary

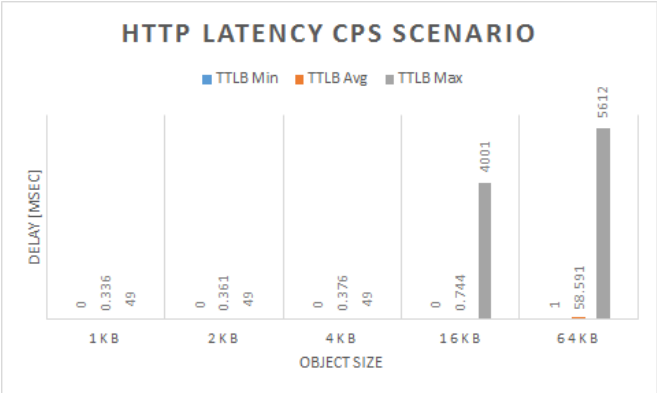


Figure 9: HTTP Transaction Latency Result Summary

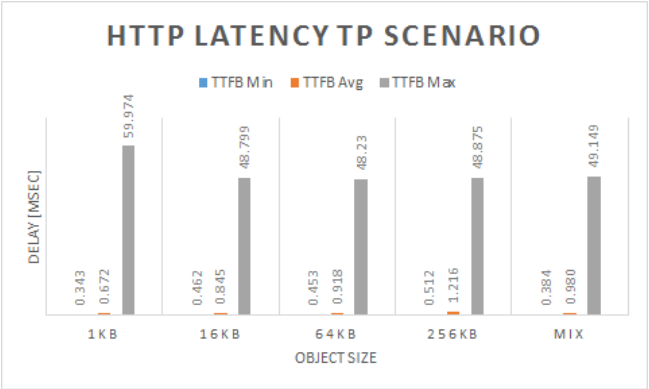


Figure 10: HTTP Transaction Latency Result Summary

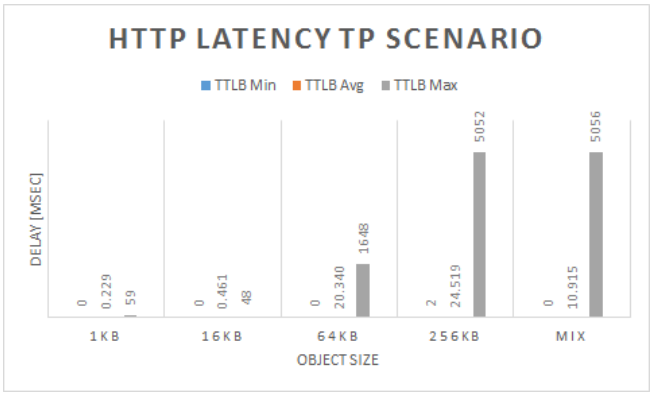


Figure 11: HTTP Transaction Latency Result Summary

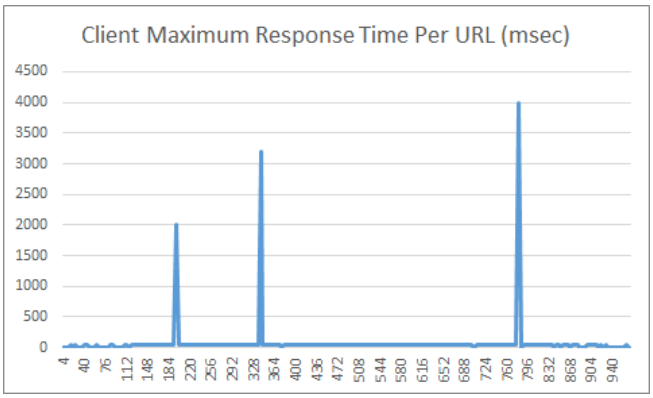


Figure 12: Overall Maximum Time to Last Byte of HTTP CPS 16K

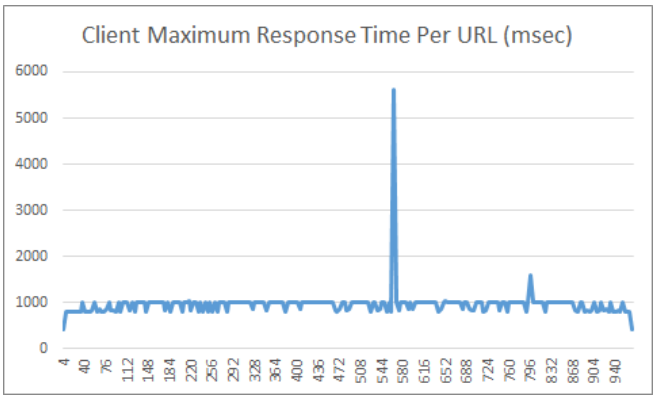


Figure 13: Overall Maximum Time to Last Byte of HTTP CPS 64K

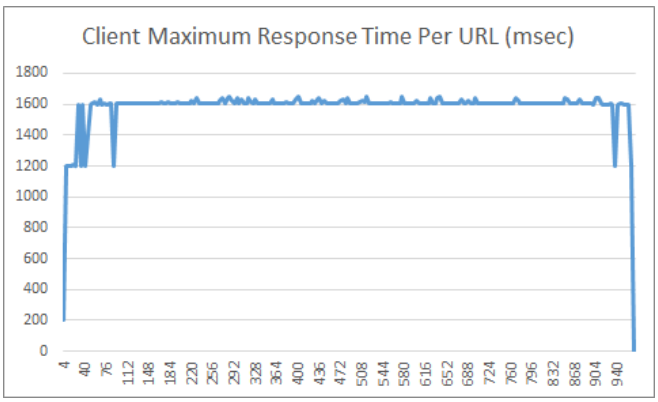


Figure 14: Overall Maximum Time to Last Byte of HTTP TP 64K

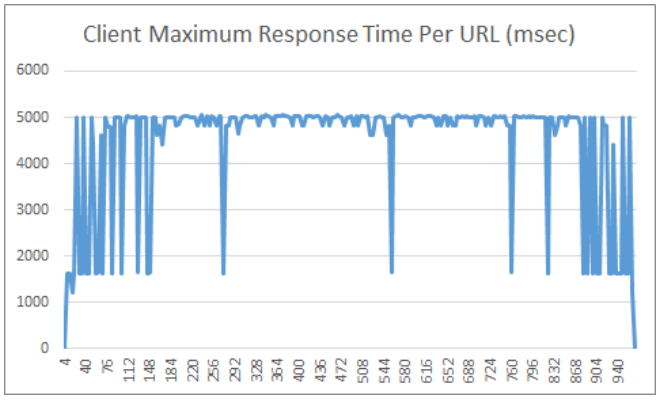


Figure 15: Overall Maximum Time to Last Byte of HTTP TP 256K

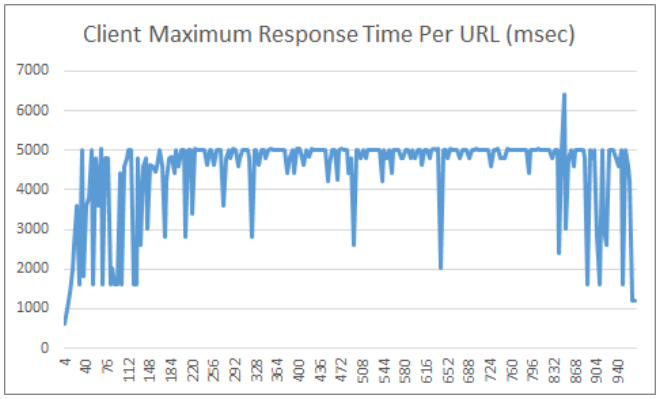


Figure 16: Overall Maximum Time to Last Byte of HTTP TP Mix

8.4. Concurrent TCP/HTTP Connection Capacity

We executed this test with Avalanche Commander 5.03. The test contained 180 s ramp-up time, 720 s sustain phase and 180 s ramp-down time. The think time is 90s. Think time is the delay time between every single transaction. We measured 1,550,000 concurrent HTTP connections in this test case. The test results met the requirements of "7.5.3.3. Test Results Validation Criteria".

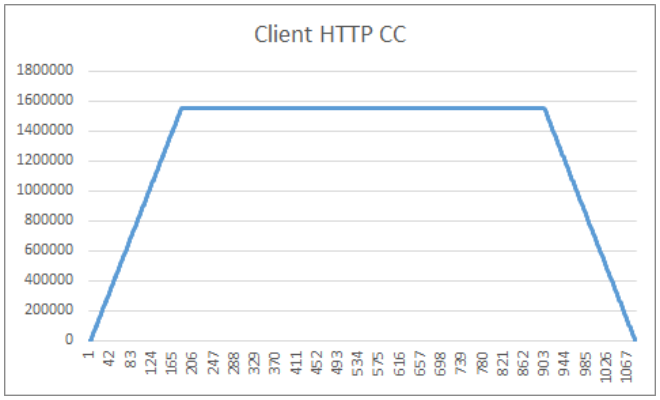


Figure 17: HTTP CC Test Result Summary

8.5. TCP/HTTPS Connections Per Second

We executed this test with Spirent automation script v1.6. We chose ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048 as our cipher suite, which is the second option of recommended ciphers and keys in the draft. The test contained 180 s ramp-up time, 600 s sustain phase and 180 s ramp-down time. All the test results met the requirements of "7.6.3.3. Test Results Validation Criteria".

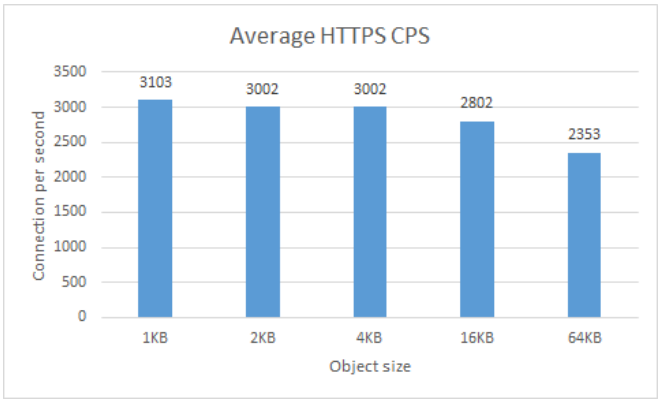


Figure 18: HTTPS CPS Test Result Summary

8.6. HTTPS Throughput

We executed this test with Spirent automation script v1.6. We chose ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048 as our cipher suite, which is the second option of recommended ciphers and keys in the draft. The test contained 180 s ramp-up time, 600 s sustain phase and 180 s ramp-down time. All the test results met the requirements of "7.7.3.3. Test Results Validation Criteria" except item c. The CC deviation was more than 10%. However, the trend of the deviation tended to be stable instead of increasing. Therefore, we evaluated the test result to meet the item c.

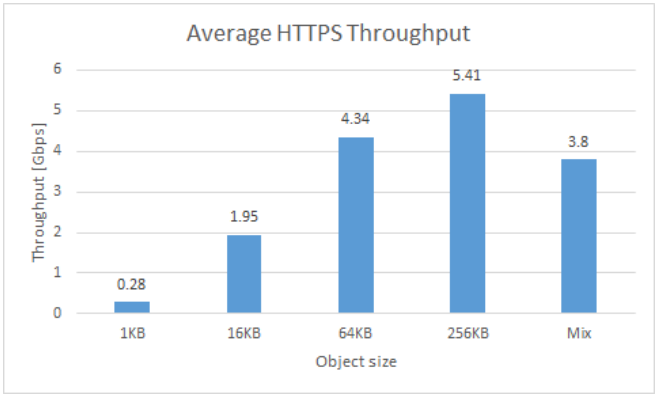


Figure 19: HTTPS Throughput Test Result Summary

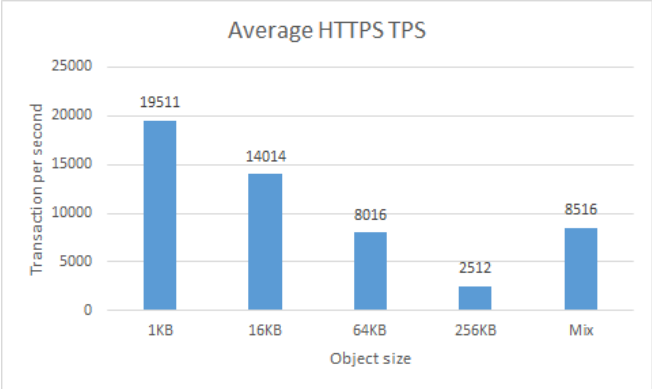


Figure 20: HTTPS Throughput Test Result Summary

8.7. HTTPS Transaction Latency

We executed this test with Spirent automation script v1.6. We chose ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048 as our cipher suite, which is the second option of recommended ciphers and keys in the draft. The test contained 180 s ramp-up time, 600 s sustain phase and 180 s ramp-down time. All the test results met the requirements of "7.8.3.3. Test Results Validation Criteria".

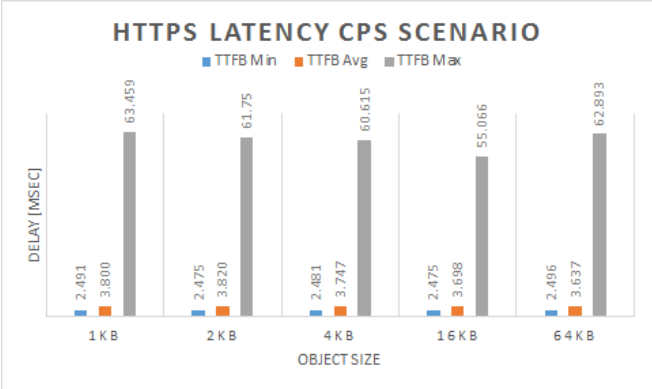


Figure 21: HTTPS Transaction Latency Test Result Summary

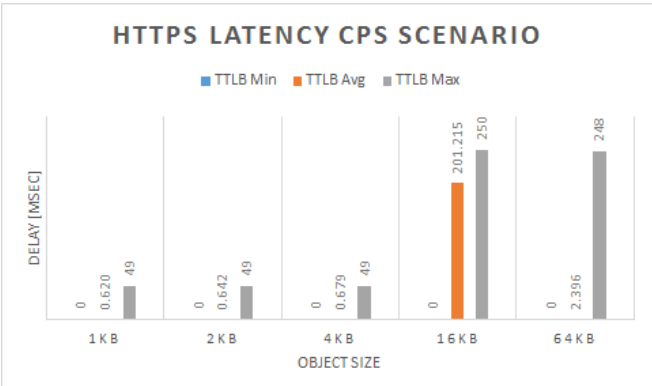


Figure 22: HTTPS Transaction Latency Test Result Summary

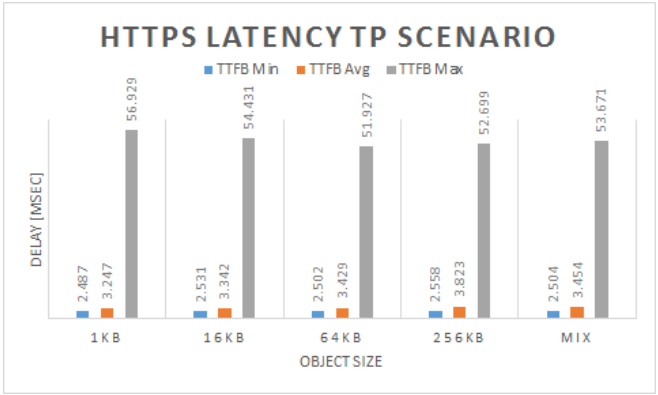


Figure 23: HTTPS Transaction Latency Test Result Summary

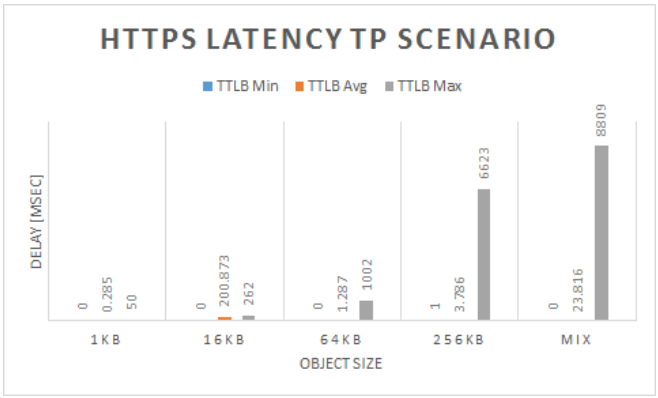


Figure 24: HTTPS Transaction Latency Test Result Summary

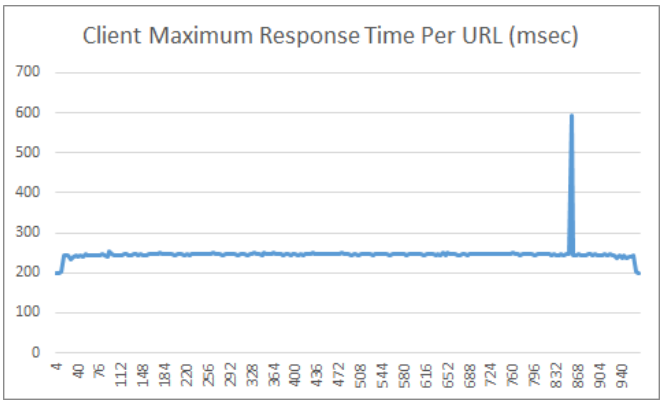


Figure 25: Overall Maximum Time to last Byte of HTTPS CPS 16K

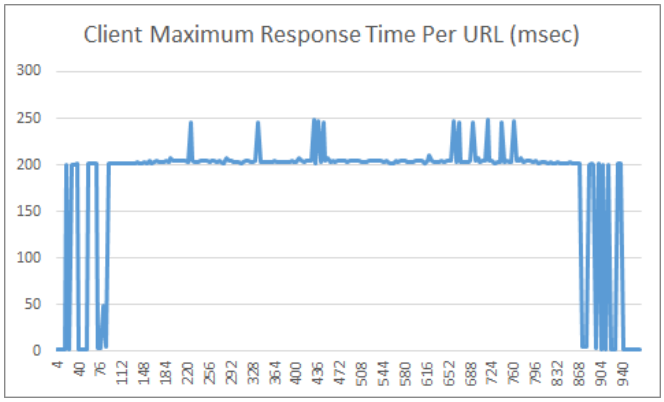


Figure 26: Overall Maximum Time to last Byte of HTTPS CPS 64K

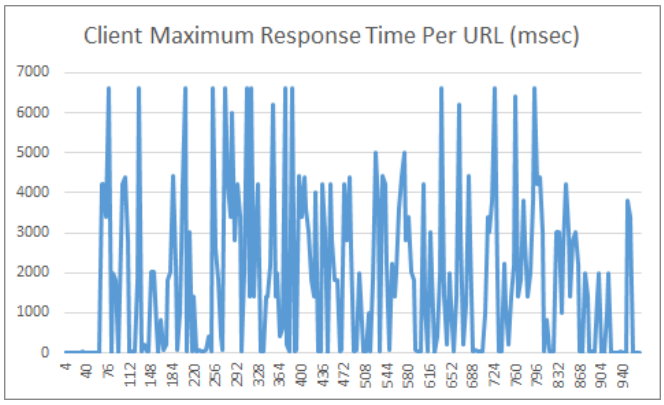


Figure 27: Overall Maximum Time to last Byte of HTTPS TP 256K

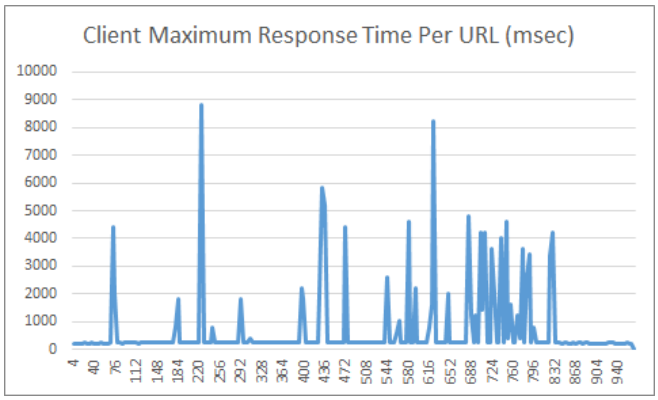


Figure 28: Overall Maximum Time to last Byte of HTTPS TP Mix

8.8. Concurrent TCP/HTTPS Connection Capacity

We executed this test with Avalanche Commander 5.03. We chose ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048 as our cipher suite which is the second option of recommended ciphers and keys in the draft. The test contained 450 s ramp-up time, 450 s sustain phase, and 450 s ramp-down time. The think time is 90 s. We measured 745,000 concurrent HTTPS connections in this test case. The test results met the requirements of "7.9.3.3. Test Results Validation Criteria".

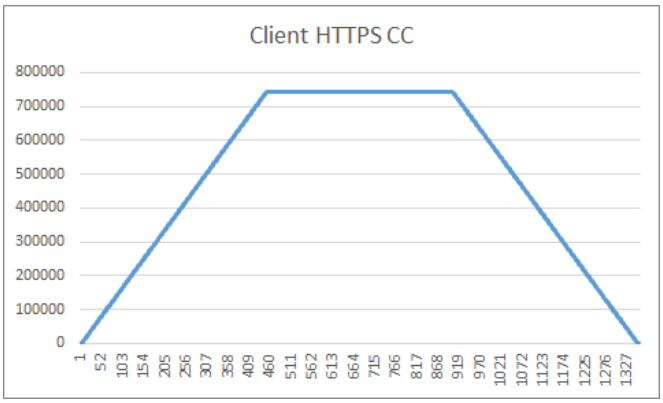


Figure 29: HTTPS CC Test Result Summary

Appendix

HTTP CPS Test Results in detail

Test Name	CPS & TPS	Avg. Total Bandwitdh (Kbps)	Avg. Concurrent connections	Avg. TCP synack time (ms)	Avg. TTFB (ms)	Avg. TTLB (ms)	Cumulative Successful Transactions	Cumulative Unsuccessful Transactions	Cumulative established TCP connections
HTTP-CPS-1K	22,432	321,326	112	2.3	4.8	2.6	17,608,715	0	17,608,715
HTTP-CPS-2K	20,503	466,526	113	2.4	5.1	2.7	16,092,169	0	16,092,169
HTTP-CPS-4K	17,107	679,054	46	1.4	3.0	1.6	13,423,995	0	13,423,995
HTTP-CPS-16K	12,471	1,740,762	83	2.1	4.4	5.0	9,790,243	0	9,790,243
HTTP-CPS-64K	6,492	3,539,134	434	1.9	4.0	65.0	5,096,531	0	5,096,531

Table 5: HTTP CPS Test Results

HTTP TP Test Results in detail

Test Name	CPS	TPS	Avg. Total Bandwitdh (Kbps)	Avg. Concurrent connections	Avg. TCP synack time (ms)	Avg. TTFB (ms)	Avg. TTLB (ms)	Cumulative Successful Transactions	Cumulative Unsuccessful Transactions	Cumulative established TCP connections
HTTP-TPUT-1K	7,593	75,931	873,038	96	1	2.2	1.1	59,605,210	0	5,960,521
HTTP-TPUT-16K	2,753	27,532	3,765,511	43	1.2	2.5	1.5	21,607,230	0	2,160,723
HTTP-TPUT-64K	953	9,517	5,112,559	186	1.2	2.4	19.4	7,468,140	0	746,814
HTTP-TPUT-256K	301	3,010	6,435,491	106	2.4	4.9	34.8	2,367,490	0	236,749
HTTP-TPUT-MIX	1,202	12,017	5,306,888	212	1.6	3.4	17.3	9,430,810	0	943,081

Table 6: HTTP TP Test Results

HTTP LAT Test Results in detail

Test Name	CPS	TPS	Avg. Total Bandwitdh (Kbps)	Avg. Concurrent connections	Avg. TCP synack time (ms)	Avg. TTFB (ms)	Avg. TTLB (ms)	Cumulative Successful Transactions	Cumulative Unsuccessful Transactions	Cumulative established TCP connections
HTTP-TPUT-LAT-1K	3,804	38,034	437,245	9	0.4	0.7	0.2	29,851,190	0	2,985,119
HTTP-CPS-LAT-1K	11,260	11,260	160,282	6	0.4	0.7	0.3	8,837,212	0	8,837,212
HTTP-TPUT-LAT-16K	1,378	13,768	1,882,951	7	0.4	0.8	0.5	10,804,810	0	1,080,481
HTTP-CPS-LAT-2K	10,231	10,231	231,898	5	0.3	0.7	0.4	8,031,651	0	8,031,651
HTTP-TPUT-LAT-64K	478	4,765	2,561,200	97	0.4	0.9	20.3	3,739,750	0	373,975
HTTP-CPS-LAT-4K	8,538	8,538	333,837	4	0.3	0.7	0.4	6,702,594	0	6,702,594
HTTP-TPUT-LAT-256K	153	1,520	3,249,850	37	0.6	1.2	24.4	1,200,540	0	120,054
HTTP-CPS-LAT-16K	6,246	6,246	871,245	6	0.3	0.8	0.7	4,902,274	0	4,902,274
HTTP-TPUT-LAT-MIX	602	6,014	2,655,391	66	0.4	1	10.9	4,719,900	0	471,990
HTTP-CPS-LAT-64K	3,255	3,254	1,782,149	194	0.3	0.8	58.6	2,553,794	0	2,553,794

Table 7: HTTP LAT Test Results

HTTP CC Test Result in detail

Test Name	CPS	TPS	Avg. Total Bandwitdh (Kbps)	Avg. Concurrent connections	Avg. TCP synack time (ms)	Avg. TTFB (ms)	Avg. TTLB (ms)	Cumulative Successful Transactions	Cumulative Unsuccess-ful Transactions	Cumulative established TCP connections
HTTP-CC - 1K	N/A	17,232	198,442	1,550,000	N/A	N/A	0.4	15,500,000	0	1,550,000

Table 8: HTTP CC Test Result

HTTPS CPS Test Results in detail

Test Name	CPS	TPS	Avg. Total Bandwitdh (Kbps)	Avg. Concurrent connections	Avg. TCP synack time (msec)	Avg. TTFB (msec)	Avg. TTLB (msec)	Cumulative Successful Transactions	Cumulative Unsuccess-ful Transactions	Cumulative established TCP connections
HTTPS-CPS-1K	3,103	3,103	100,481	85	5.8	16	4.7	2,435,173	0	2,435,173
HTTPS-CPS-2K	3,002	3,002	122,518	70	4.2	12.8	3.3	2,355,968	0	2,355,968
HTTPS-CPS-4K	3,002	3,002	173,376	73	4.7	13.6	3.9	2,356,125	0	2,356,125
HTTPS-CPS-16K	2,802	2,802	441,789	63	3.5	11.1	3.3	2,199,299	0	2,199,299
HTTPS-CPS-64K	2,353	2,352	1,313,376	57	3.4	10.2	9	1,846,292	0	1,846,292

Table 9: HTTPS CPS Test Results

HTTPS TP Test Results in detail

Test Name	CPS	TPS	Avg. Total Bandwitdh (Kbps)	Avg. Concurrent connections	Avg. TCP synack time (ms)	Avg. TTFB (ms)	Avg. TTLB (ms)	Cumulative Successful Transactions	Cumulative Unsuccessful Transactions	Cumulative established TCP connections
HTTPS-TPUT-1K	1,951	19,511	277,072	44	1.5	6.1	1.1	15,313,960	0	1,531,396
HTTPS-TPUT-16K	1,402	14,014	1,954,597	2,857	1.9	6.6	203	10,998,870	0	1,099,887
HTTPS-TPUT-64K	802	8,016	4,336,573	64	3.1	9.2	6.7	6,290,450	0	629,045
HTTPS-TPUT-256K	252	2,512	5,407,987	58	2	7.1	21.8	1,977,520	0	197,752
HTTPS-TPUT-MIX	852	8,516	3,798,272	248	2.9	8.6	27.8	6,682,970	0	668,297

Table 10: HTTPS TP Test Results

HTTPS LAT Test Results in detail

Test Name	CPS	TPS	Avg. Total Bandwitdh (Kbps)	Avg. Concurrent connections	Avg. TCP synack time (ms)	Avg. TTFB (ms)	Avg. TTLB (ms)	Cumulative Successful Transactions	Cumulative Unsuccessful Transactions	Cumulative established TCP connections
HTTPS-TPUT-LAT-1K	978	9,766	138,673	9	0.4	3.2	0.3	7,664,150	0	766,415
HTTPS-CPS-LAT-1K	1,552	1,552	50,868	12	0.6	3.8	0.6	1,217,862	0	1,217,862
HTTPS-TPUT-LAT-16K	703	7,015	978,403	1,413	0.4	3.3	200.9	5,505,400	0	550,540
HTTPS-CPS-LAT-2K	1,503	1,502	61,898	12	0.7	3.8	0.6	1,178,683	0	1,178,683
HTTPS-TPUT-LAT-64K	403	4,016	2,168,844	8	0.5	3.4	1.3	3,151,920	0	315,192
HTTPS-CPS-LAT-4K	1,502	1,502	86,566	12	0.6	3.7	0.7	1,178,518	0	1,178,518
HTTPS-TPUT-LAT-256K	127	1,263	2,708,482	6	0.7	3.8	3.8	1,000,240	0	100,024
HTTPS-CPS-LAT-16K	1,402	1,402	221,513	291	0.6	3.7	201.2	1,100,017	0	1,100,017
HTTPS-TPUT-LAT-MIX	428	4,264	1,896,260	105	0.5	3.4	23.8	3,347,500	0	334,750
HTTPS-CPS-LAT-64K	1,178	1,177	657,334	11	0.6	3.6	2.4	923,433	0	923,433

Table 11: HTTPS LAT Test Results

HTTPS CC Test Result in detail

Test Name	CPS	TPS	Avg. Total Bandwitdh (Kbps)	Avg. Concurrent connections	Avg. TCP synack time (ms)	Avg. TTFB (ms)	Avg. TTLB (ms)	Cumulative Successful Transactions	Cumulative Unsuccessful Transactions	Cumulative established TCP connections
HTTP-CC -1K	N/A	8,270	103,063	745,000	N/A	N/A	0.6	7,440,470	0	745,000

Table 12: HTTPS CC Test Result

CVE Detection Rates

As stated previously, we performed the CVE check to verify the security functionality of the DUT during the performance test. Two vulnerability sets were used, one Public and one Private. (The private set was not known to the DUT vendor in order to ensure the test was not being gamed.) The public set contained approximately 435 CVEs and the private set contained approximately 30 CVEs.

As a preview to the security effectiveness test methodology under development, following are the respective private and public block rates used to verify security functionalities/modules are engaged.

The block rates for this test are:

- Public CVE block rate: 410 out of 436 (94.03%)
- Private CVE block rate: 31 out of 33 (93.93%)

About Fortinet NGFW

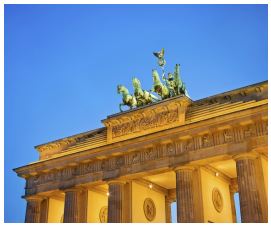
Fortinet explained that FortiGate Next-Generation Firewalls (NGFWs) utilize purpose-built security processors and threat intelligence security services from AI-powered FortiGuard labs to deliver top-rated protection, high performance inspection of clear-texted and encrypted traffic. Next-generation firewalls reduce cost and complexity with full visibility into applications, users and networks, and provides the best of breed security. As an integral part of the Fortinet Security Fabric, next-generation firewalls can communicate within Fortinet's comprehensive security portfolio as well as third-party security solutions in a multivendor environment to share threat intelligence and improve security posture.

Fortinet further mentioned that the FortiGate 500E series delivers next-generation firewall capabilities for mid-sized to large enterprises, with the flexibility to be deployed at the campus or enterprise branch. It protects against cyber threats with security processor powered high performance, security efficacy and deep visibility.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 425,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

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.