Fortinet FortiGate 601F NetSecOPEN report

Chao Guo
EANTC AG
1/2/24

1. Introduction

Date of test: December 2023

Place of test: Berlin, Germany

2. Summary of the test bed software and hardware details

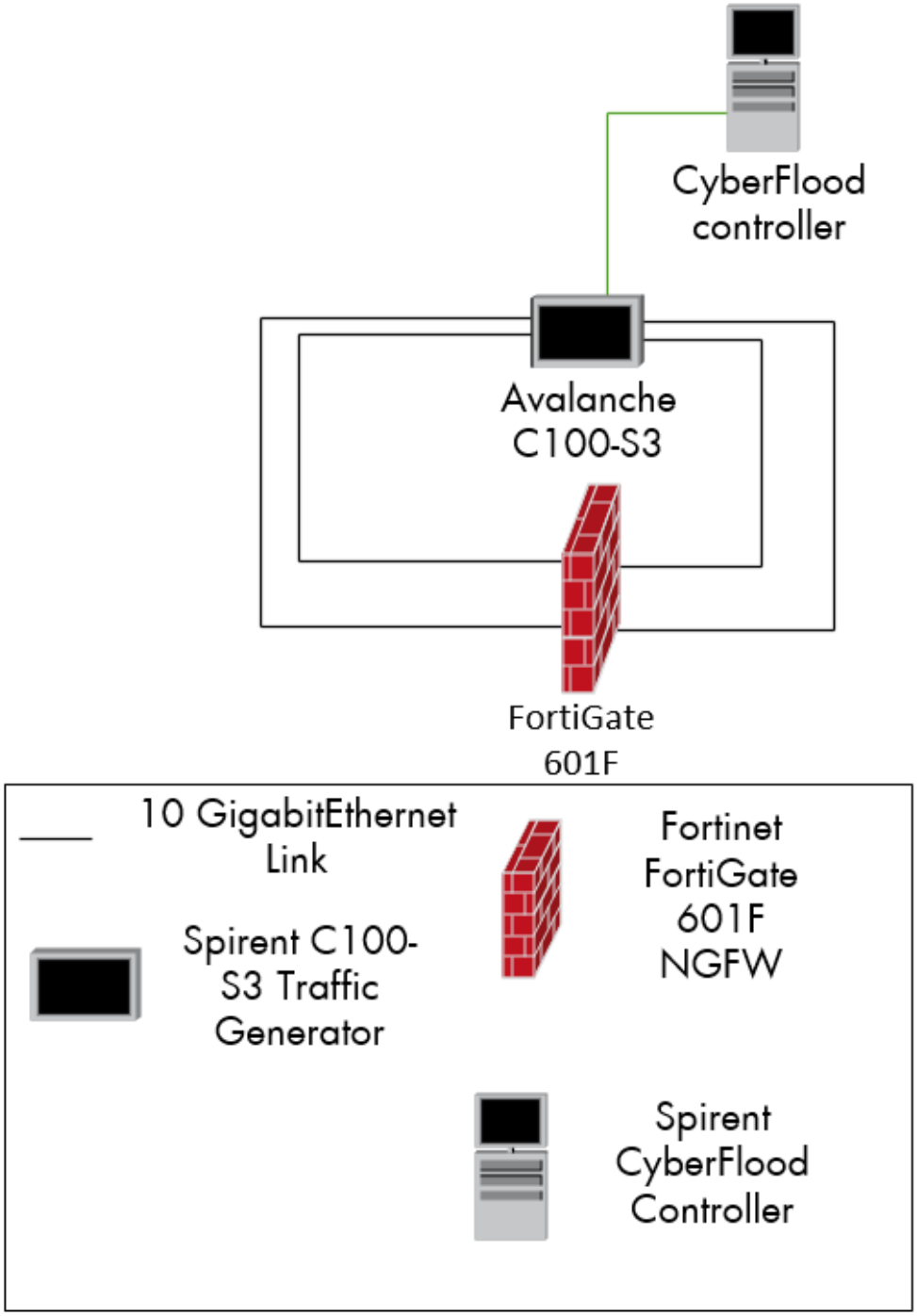


Figure 1. Testbed Setup

2.1 DUT hardware info

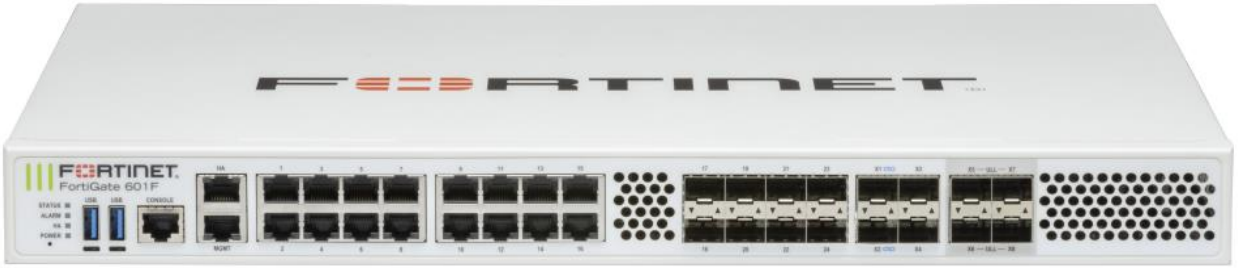


Figure 2. DUT front panel

Description	Info
DUT vendor	Fortinet
DUT hardware and model	FortiGate 601F
DUT security working mode	NAT
Tested interface type, SFP, and speed	X3 and x4, 10G SFP+
Additional hardware component	N/A

Table 1. DUT hardware info

2.2 DUT/SUT software info

Description	Info
DUT OS	FortiOS
DUT OS version	v7.2.6,build1575,230926 (GA.F)
IPS/IDS definition	IPS-DB: 6.00741 IPS-ETDB: 26.00689
Anti-Spyware definition	N/A
Anti-Virus definition	Virus-DB: 91.09456 Extended DB: 91.09456 Extreme DB: 91.09266
Anti-Botnet definition	7.03483
Anti-Evasion definition	N/A
Web Filtering definition	4.00899
Data Loss Protection (DLP) definition	N/A
Deep Packet Inspection (DPI) definition	N/A
DDoS Protection definition	N/A
Certificate Validation definition	1.00457
Logging and Reporting definition	N/A
Application Identification definition	26.00689
Additional hardware component software version	N/A

Table 2. DUT/SUT software info

2.3 DUT/SUT enabled features

DUT/SUT Features	Recommended	Status
Anti-Botnet	Yes	Yes
Anti-Virus	Yes	Yes

Anti-Spyware	Yes	Yes
Application Identification	Yes	Yes
Certificate Validation	No	Yes
Data Loss Protection (DLP)	No	No
DDoS Protection	No	No
IDS/IPS	Yes	Yes
Logging and Reporting	Yes	Yes
TLS Inspection	Yes	Yes
Web Filtering	No	No

Table 3. NGFW Security Features

2.4 Test equipment hardware and software

Description	Info
Test equipment vendor	Spirent
Test equipment hardware model	C100-S3-MP-2
Chassis OS version	5.44.3243
Avalanche Commander version	5.44 build 1076 64bit
Cyberflood controller version	23.7.1006 with 1 customized patch
Tested interface type, SFP, and speed	1 and 2, 10G SPF+

Table 4. Spirent hardware and software info

2.5 Key test parameters

Name and version of the standard: RFC9411

Used cipher suites and keys: ECDHE-ECDSA-AES128-GCM-SHA256 with Prime256v1 (Signature Hash Algorithm: ecdsa_secp256r1_sha256 and Supported group: secp256r1)

IPv4 and IPv6 traffic distribution: IPv4:IPv6 = 100:0

Client and server IP address:

IP address	Count
Client	
198.18.16.0/21	750
198.18.24.0/21	750
Server	
198.18.32.0/21	750
198.18.40.0/21	750

Table 5. Client and server IP addresses

DUT class:

Rules Type	Match Criteria	Description	Action	DUT/SUT classification Rules			
				XS	S	M	L
Application layer	Application	Any application not included in the measurement traffic	block	N/A			50

Transport layer	SRC IP and TCP/UDP DST ports	Any SRC IP prefix used and any DST ports not used in the measurement traffic	block		250
IP layer	SRC/DST IP	Any SRC/DST IP subnet not used in the measurement traffic	block		250
Application layer	Application	Half of the applications included in the measurement traffic	allow		13
Transport layer	SRC IP and TCP/UDP DST ports	Half of the SRC IPs used and any DST ports used in the measurement traffic (one rule per subnet)	allow		4
IP layer	SRC/DST IP	The rest of the SRC IP prefix range used in the measurement traffic (one rule per subnet)	allow		1

Table 6. Number of configured ACL

TCP parameter	Value
Maximum segment size (MSS)	1460 bytes
Receive window size	65535 bytes
Initial congestion window	10 MSS
Delayed ACKs size	14600 bytes
Delayed ACKs time out	200ms
TCP retry	3
TCP push flag	Enable
TCP source port range	1024 - 65535

Table 7. TCP stack parameter

2.6 Details of application traffic mix used in the benchmarking test "Throughput Performance with Application Traffic Mix"

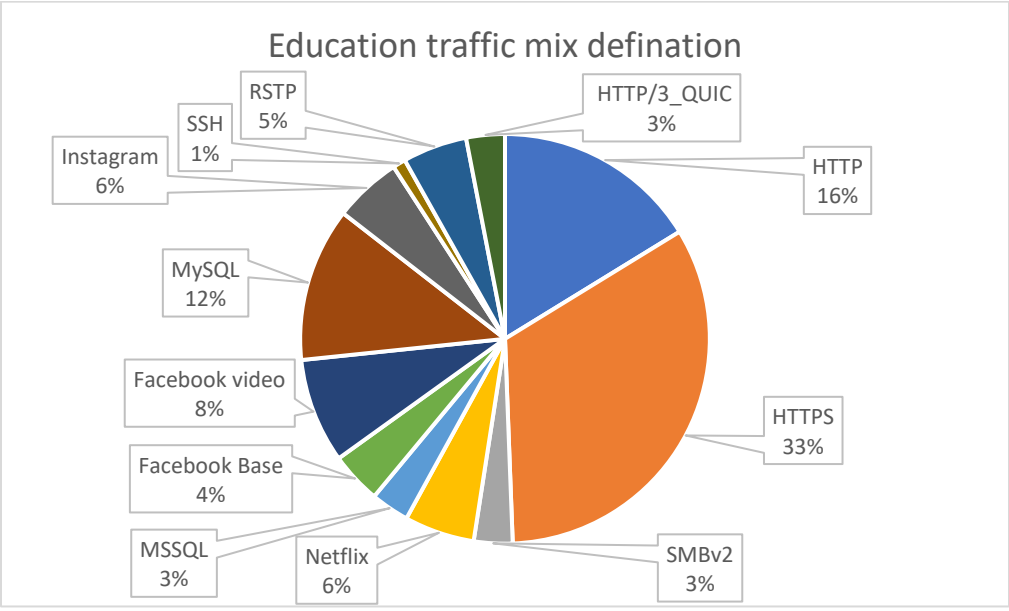


Figure 3 Education traffic mix definition

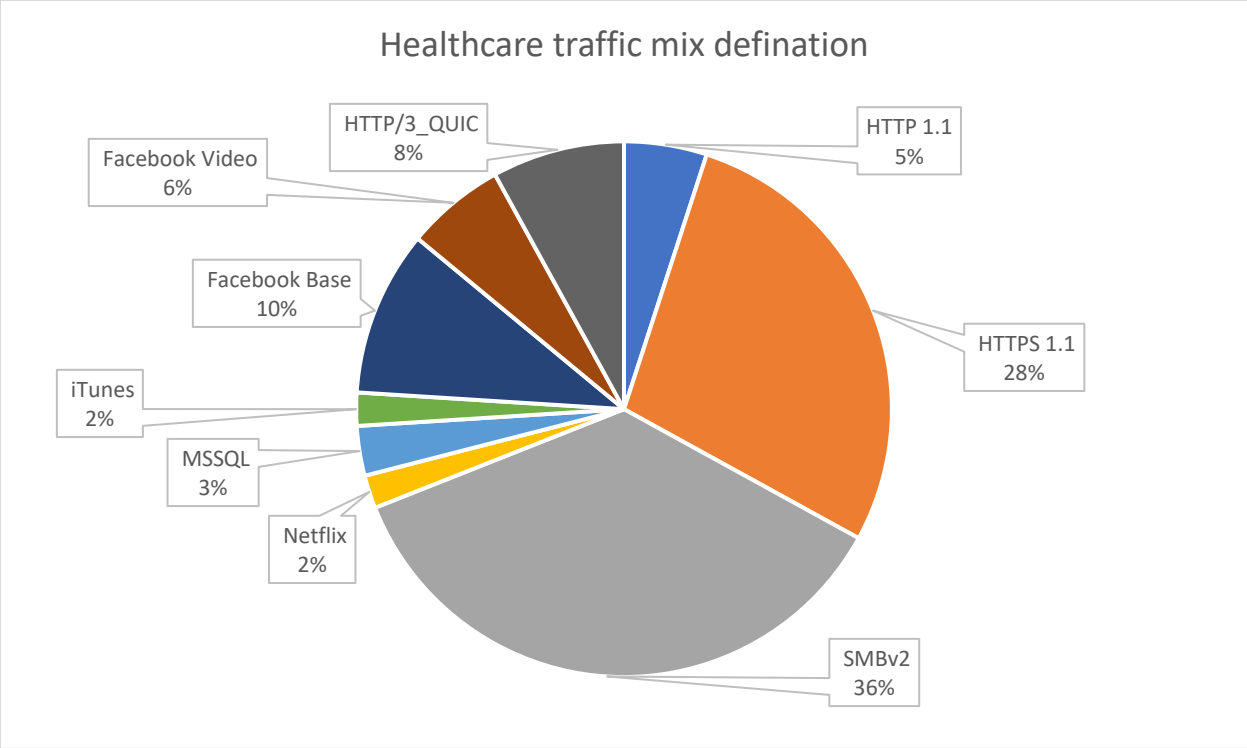


Figure 4 Healthcare traffic mix definition

3. Result Summary

3.1 Throughput Performance with Application Traffic Mix

NetSecOPEN introduces the vertical traffic mix to verify the DUT's performance in the real world. Currently, we have 2 traffic mixes: education and healthcare. We tested both traffic mixes with DUT.

The following is the result.

Application	Inspected throughput (Mbits/s)	Actual percentage	Expected percentage (± 2%)
HTTP	129.63	16.24%	16%
HTTPS	264.66	33.16%	35%
SMBv2	24.37	3.05%	3%
Netflix	44.24	5.54%	5%
MSSQL	24.24	3.04%	3%
Facebook Base	32.35	4.05%	4%
Facebook video	66	8.27%	8%
MySQL	97.04	12.16%	12%
Instagram	42.66	5.34%	5%
SSH	8.09	1.01%	1%
RSTP	40.59	5.09%	5%
HTTP/3_QUIC	24.34	3.05%	3%
Total	798.21	100%	100%

Table 8 Education traffic mix test result

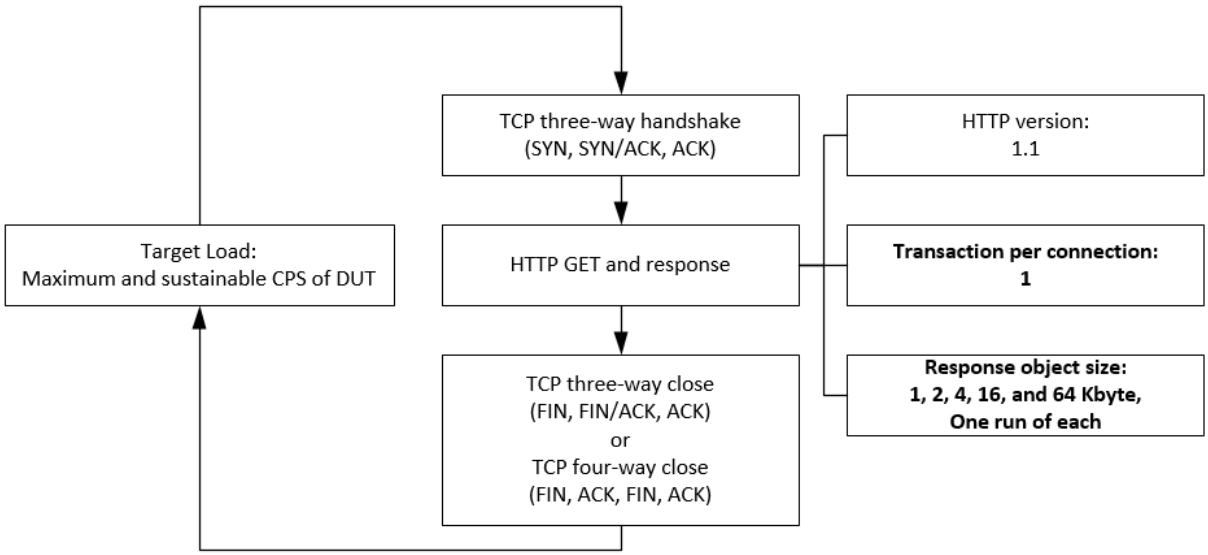
Application	Inspected throughput (Mbits/s)	Actual percentage	Expected percentage (± 2%)
HTTP	40.6	5.02%	5%
HTTPS	226.28	27.98%	28%
SMBv2	291.09	35.99%	36%
Netflix	14.98	1.85%	2%
MSSQL	24.25	3.00%	3%
iTunes	16.48	2.04%	2%
Facebook Base	80.87	10.00%	10%
Facebook Video	49.54	6.13%	6%
HTTP/3_QUIC	64.72	8.00%	8%
Total	808.81	100%	100%

Table 9 Healthcare traffic mix test result

Number	Test result validation criteria	Verdict
1	The number of failed application transactions MUST be less than 0.001% (1 out of 100,000 transactions) of the attempted transactions.	Pass
2	The number of terminated TCP connections due to unexpected TCP RST sent by the DUT/SUT MUST be less than 0.001% (1 out of 100,000 connections) of the total initiated TCP connections.	Pass
3	If HTTP/3 is used, the number of failed QUIC connections due to unexpected HTTP/3 error codes MUST be less than 0.001% (1 out of 100,000 connections) of the total initiated QUIC connections.	Pass

Table 10 Test results validation criteria

3.2 TCP/HTTP and HTTPS Connections Per Second (CPS)



This test case is to measure the maximum and sustainable TCP CPS of the DUT with HTTP traffic. We have 5 different object sizes to verify the DUT CPS performance under different traffic loads. We configured 1 transaction per TCP connection and iterated 5 times for 5 object sizes. The ramp-up phase is 180 seconds, the sustain phase is 600 seconds, and the ramp-down phase is 180 seconds.

We also run the same test for HTTPS because more traffic is encrypted in the real-world network. HTTP and TCP parameters are the same as the HTTP CPS test. We add TLS to encrypt the traffic. The DUT has enabled full SSL/TLS inspection (not only certification validation). We can verify the DUT's decrypt engine performance. The ramp-up phase is 180 seconds, the sustain phase is 600 seconds, and the ramp-down phase is 180 seconds.

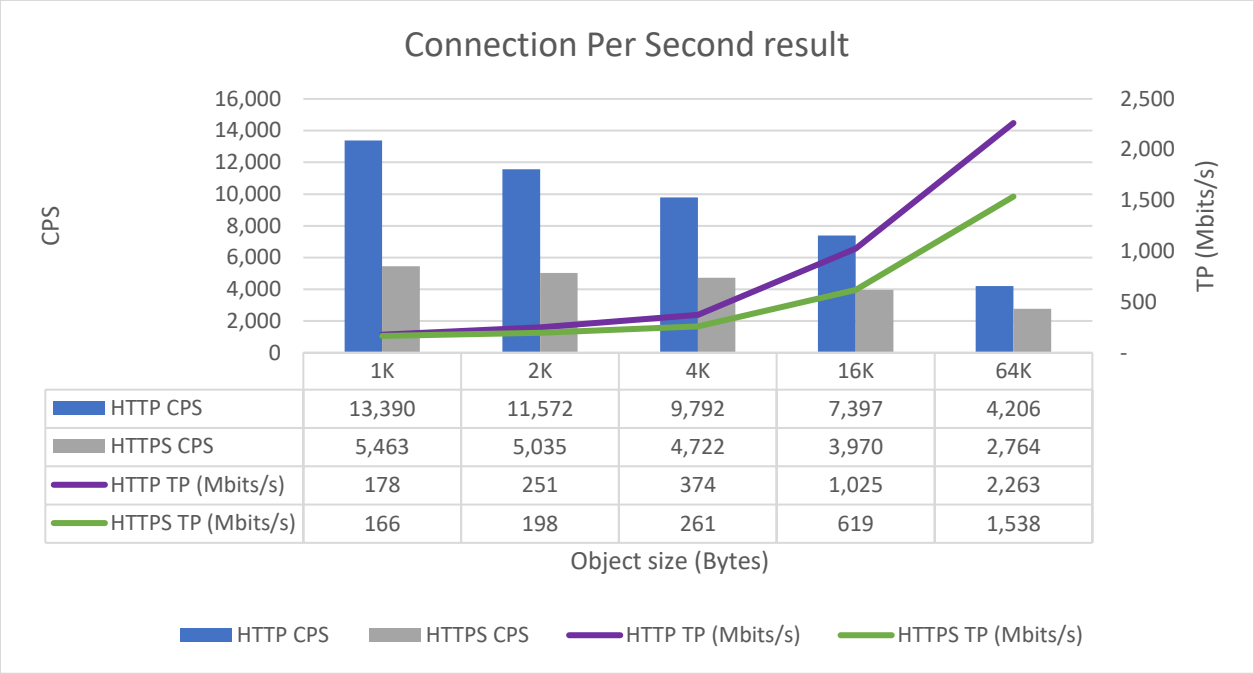


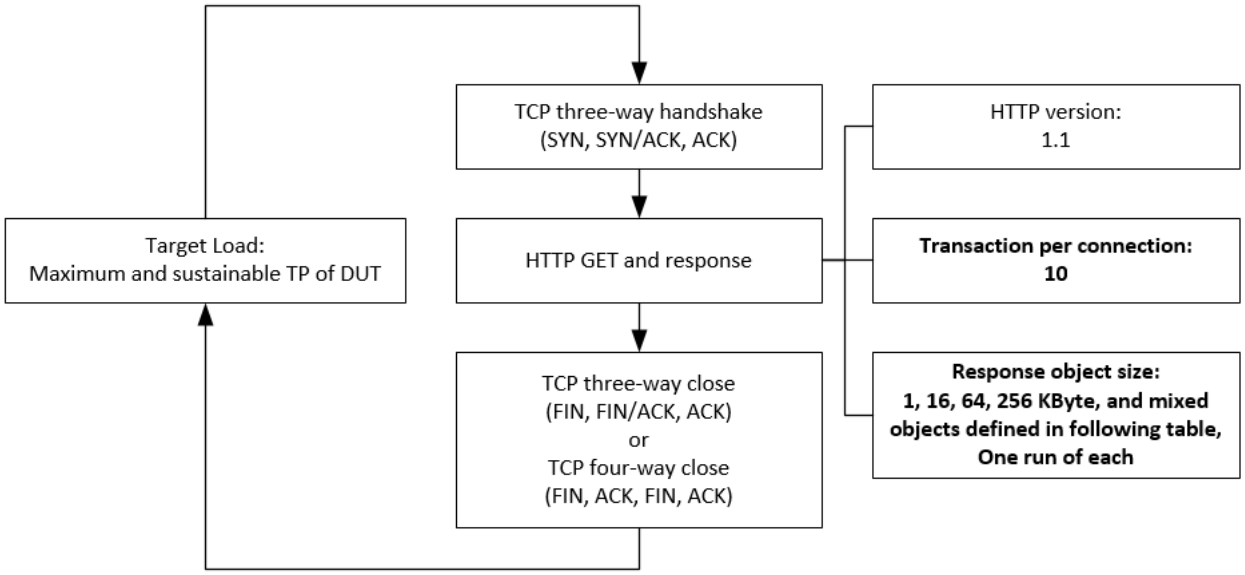
Figure 5. HTTP and HTTPS Connection Per Second (CPS) result

Number	Test result validation criteria	Verdict
1	The number of failed application transactions (receiving any HTTP response code other than 200 OK) MUST be less than 0.001% (1 out of 100,000 transactions) of total attempted transactions.	Pass
2	The number of terminated TCP connections due to unexpected TCP RST sent by DUT/SUT MUST be less than 0.001% (1 out of 100,000 connections) of total initiated TCP connections.	Pass
3	During the sustain phase, traffic MUST be forwarded at a constant rate (considered as a constant rate if any deviation of traffic forwarding rate is less than 5%).	Pass
4	Concurrent TCP connections MUST be constant during steady state and any deviation of concurrent TCP connections MUST be less than 10%. This confirms the DUT opens and closes TCP connections at approximately the same rate.	Pass[1]

Table 11. Test results validation criteria

1. The Concurrent Connection (CC) spiked during the sustain phase, but the trend tended to be stable. For example, if DUT has an average CC of 10, a 10% deviation is 1. It usually is not possible to control the CC within 9-11. However, if the CC spikes in a range bigger than 10% but in an acceptable and stable range, and DUT doesn't have unexpected behavior, we consider it a pass.

3.3 HTTP and HTTPS Throughput (TP)



Object size (KByte)	Number of requests/Weight
0.2	1
6	1
8	1
9	1
10	1
25	1
26	1
35	1
59	1
347	1

Table 12. Mixed Objects detail

This test case is to measure the maximum and sustainable TP of the DUT with HTTP and HTTPS traffic. We have 5 different object sizes to verify the DUT TP performance under different traffic loads. We configured 10 transactions per TCP connection and iterated 5 times for 5 object sizes. The ramp-up phase is 180 seconds, the sustain phase is 600 seconds, and the ramp-down phase is 180 seconds.

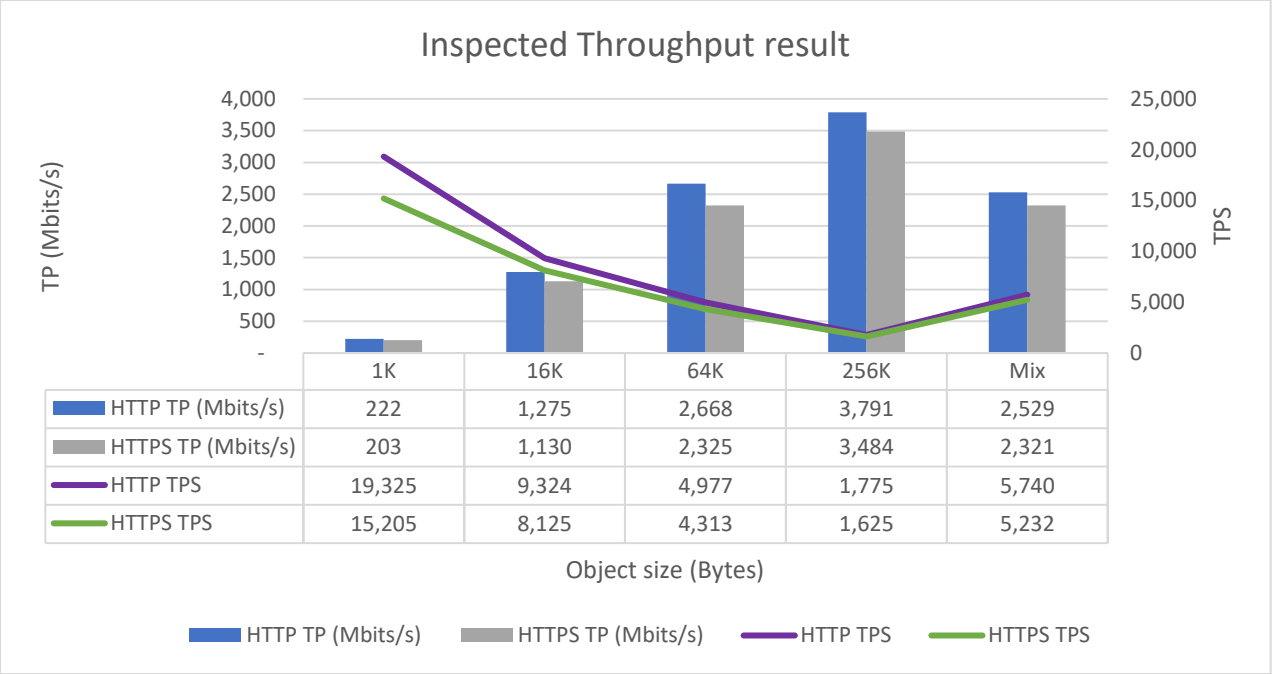


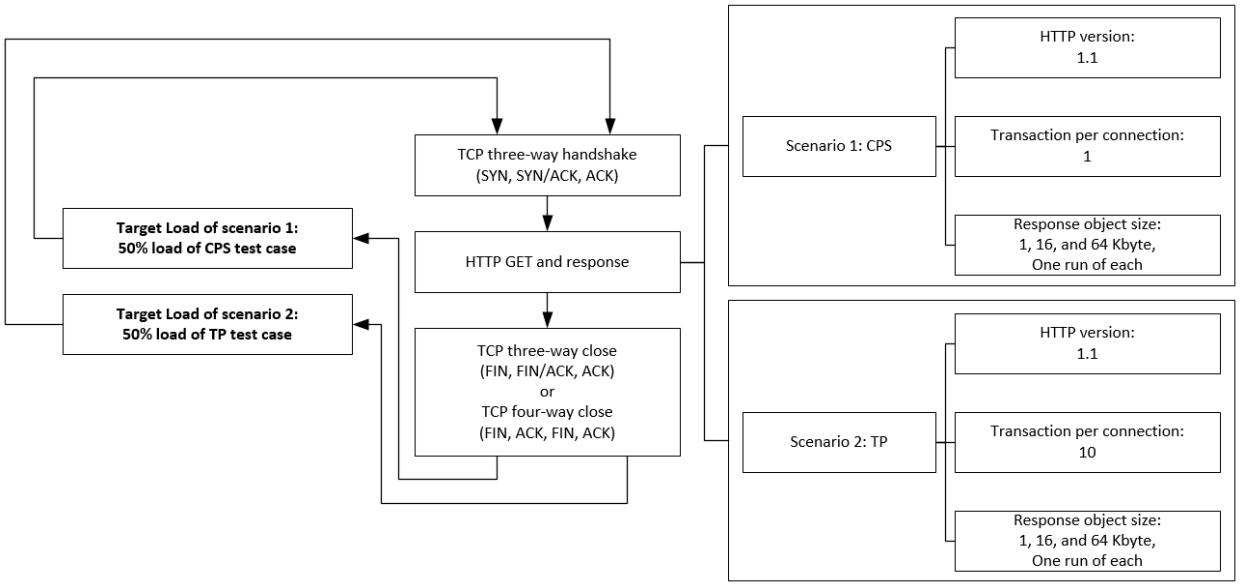
Figure6 HTTP Throughput (TP) result (TPS: Transaction Per Second)

Number	Test result validation criteria	Verdict
1	The number of failed application transactions (receiving any HTTP response code other than 200 OK) MUST be less than 0.001% (1 out of 100,000 transactions) of total attempted transactions.	Pass
2	Traffic MUST be forwarded at a constant rate (considered as a constant rate if any deviation of traffic forwarding rate is less than 5%).	Pass
3	Concurrent TCP connections MUST be constant during steady state and any deviation of concurrent TCP connections MUST be less than 10%. This confirms the DUT opens and closes TCP connections at approximately the same rate.	Pass[1]

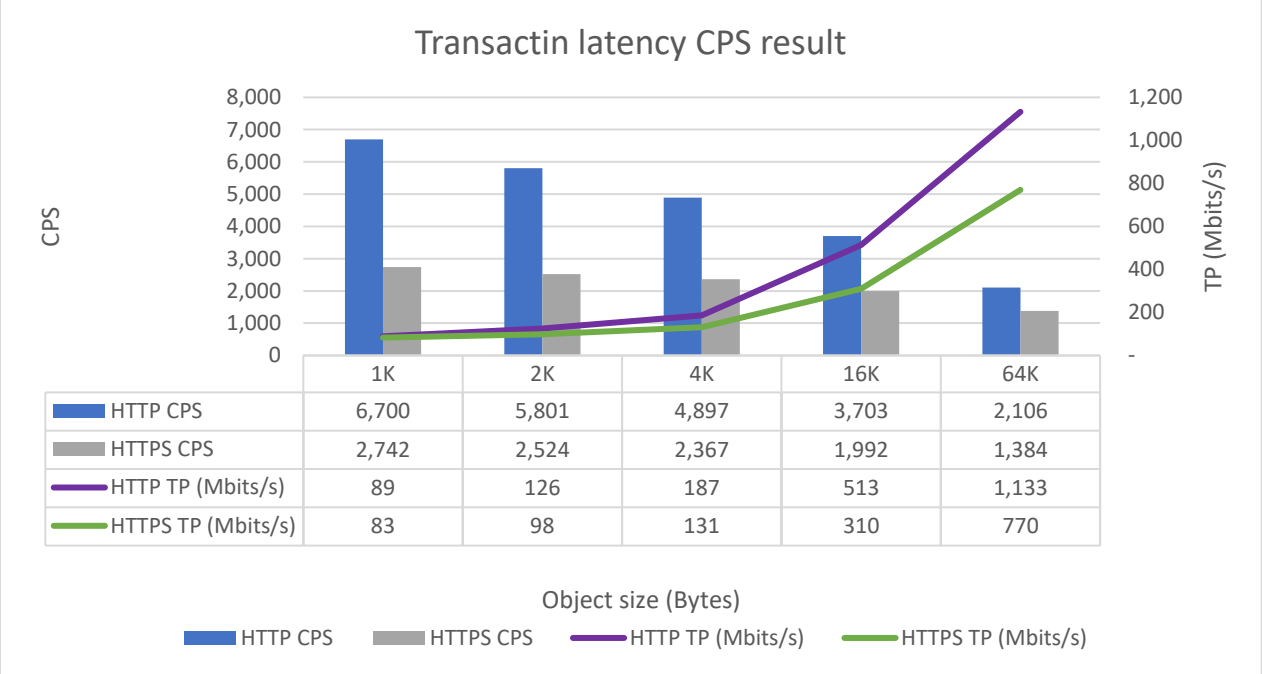
Table 13. Test results validation criteria

1. Refer to 1 under table 11.

3.4 HTTP and HTTPS Transaction Latency (TL)

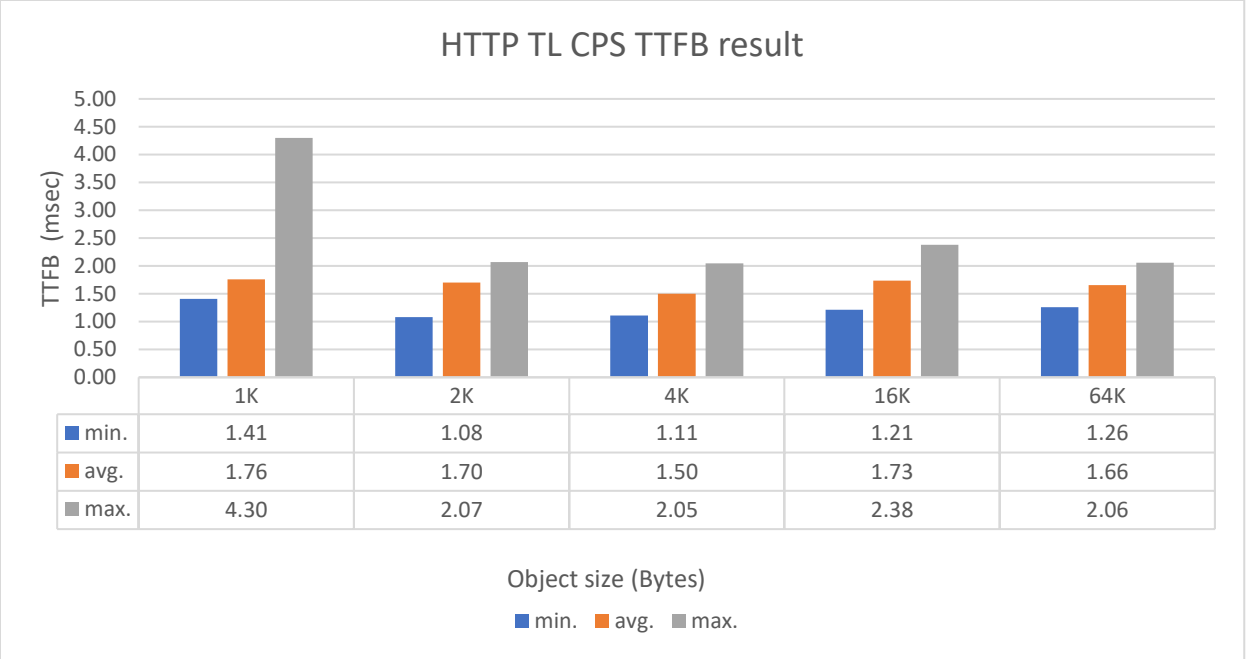


This test case is to measure the Time to First Byte (TTFB) and Time to Last Bytes (TTLB) when the DUT works with 50% of the load we measured in previous CPS and TP tests. Most customers don't usually use their device under high load (>90%). Therefore, 50% of the load condition fits most customer use cases. Consequently, we measured the latency under 50% of the maximum sustain load to determine the DUT's latency. It covers both CPS and TP scenarios, HTTP and HTTPS. The ramp-up phase is 180 seconds, the sustain phase is 600 seconds, and the ramp-down phase is 180 seconds.



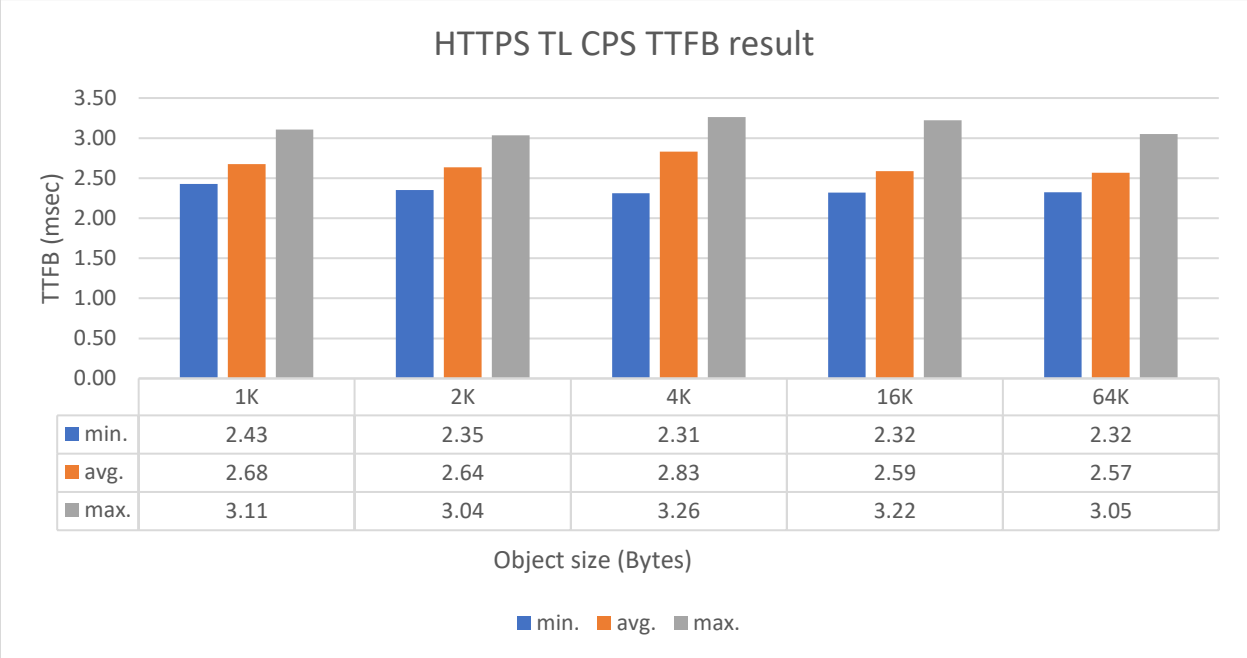
	1K	2K	4K	16K	64K
HTTP CPS	6,700	5,801	4,897	3,703	2,106
HTTPS CPS	2,742	2,524	2,367	1,992	1,384
HTTP TP (Mbits/s)	89	126	187	513	1,133
HTTPS TP (Mbits/s)	83	98	131	310	770

Figure 7 Transaction Latency (TL) CPS result



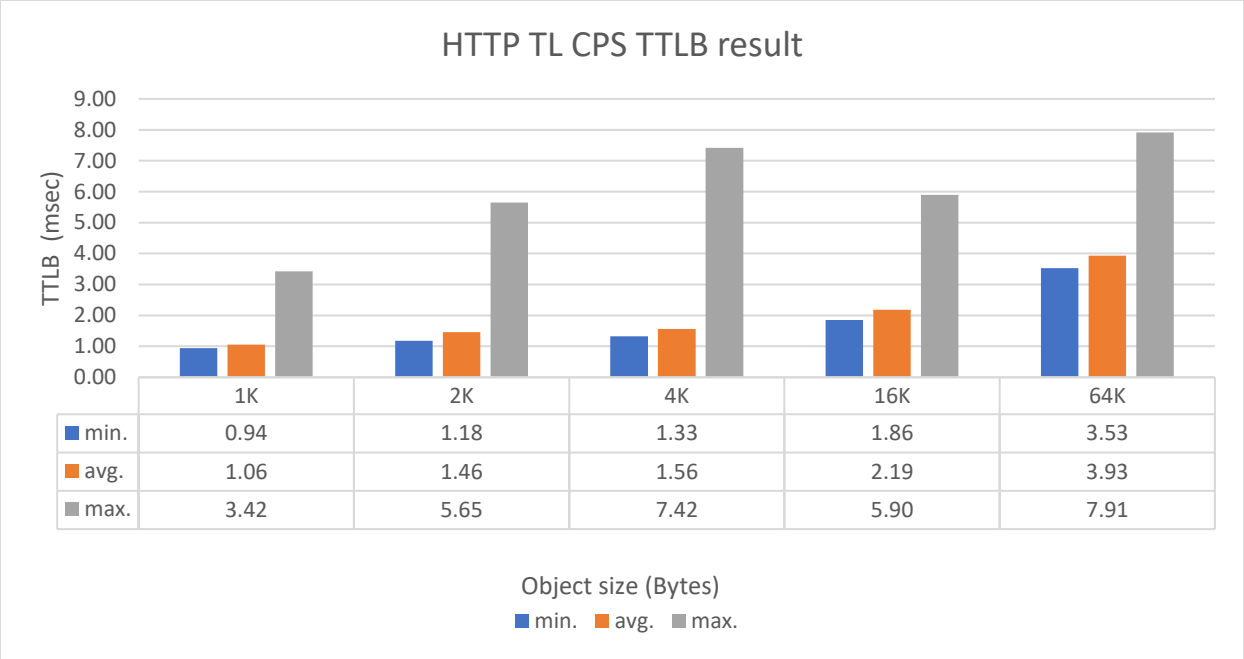
	1K	2K	4K	16K	64K
min.	1.41	1.08	1.11	1.21	1.26
avg.	1.76	1.70	1.50	1.73	1.66
max.	4.30	2.07	2.05	2.38	2.06

Figure 8 HTTP TL CPS TTFB result



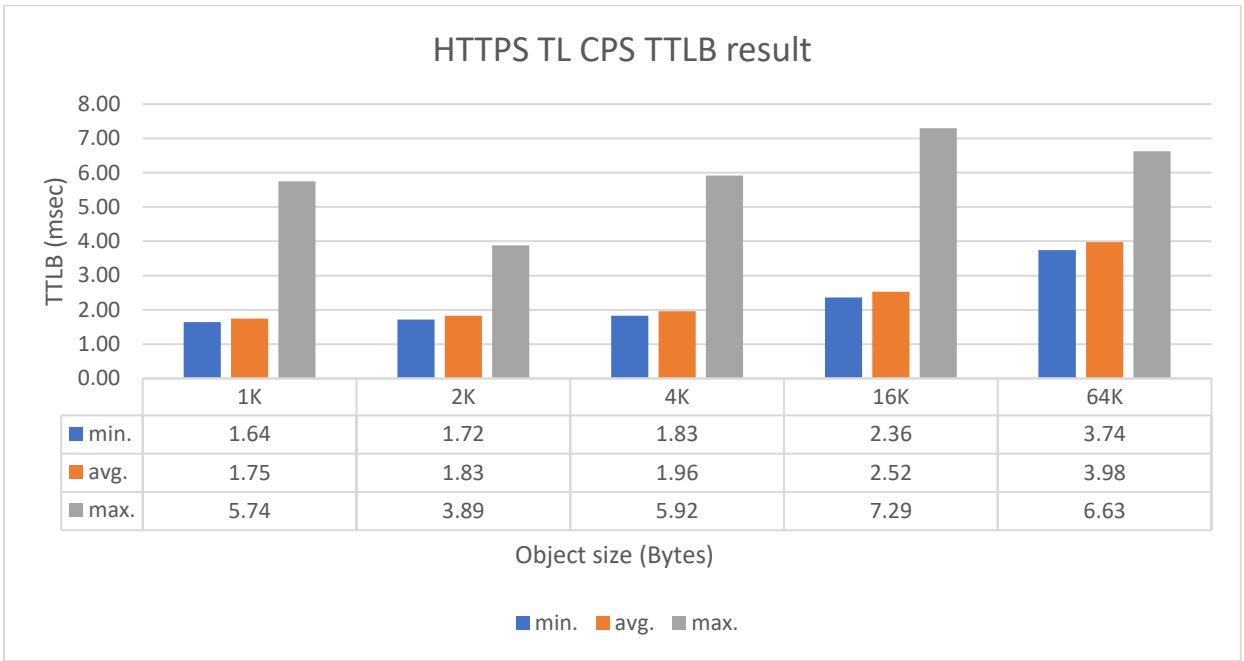
	1K	2K	4K	16K	64K
min.	2.43	2.35	2.31	2.32	2.32
avg.	2.68	2.64	2.83	2.59	2.57
max.	3.11	3.04	3.26	3.22	3.05

Figure 9 HTTPS TL CPS TTFB result



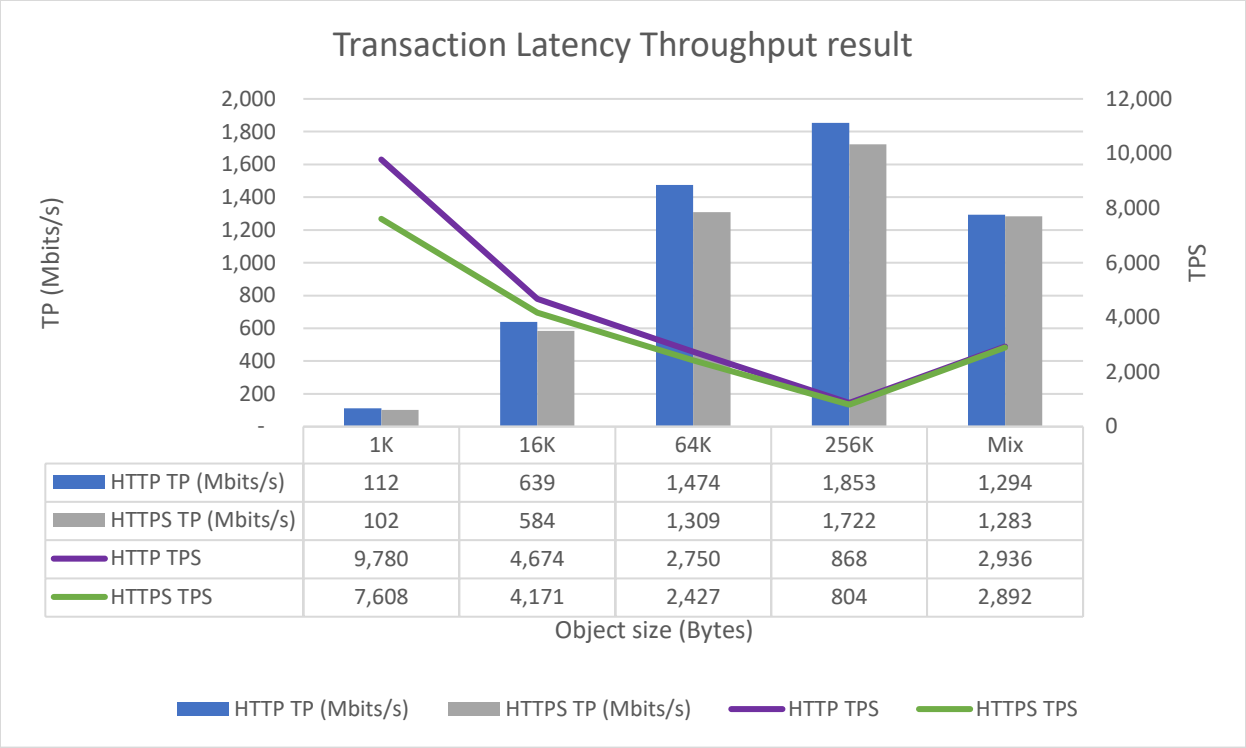
	1K	2K	4K	16K	64K
min.	0.94	1.18	1.33	1.86	3.53
avg.	1.06	1.46	1.56	2.19	3.93
max.	3.42	5.65	7.42	5.90	7.91

Figure 10 HTTP TL CPS TTLB result



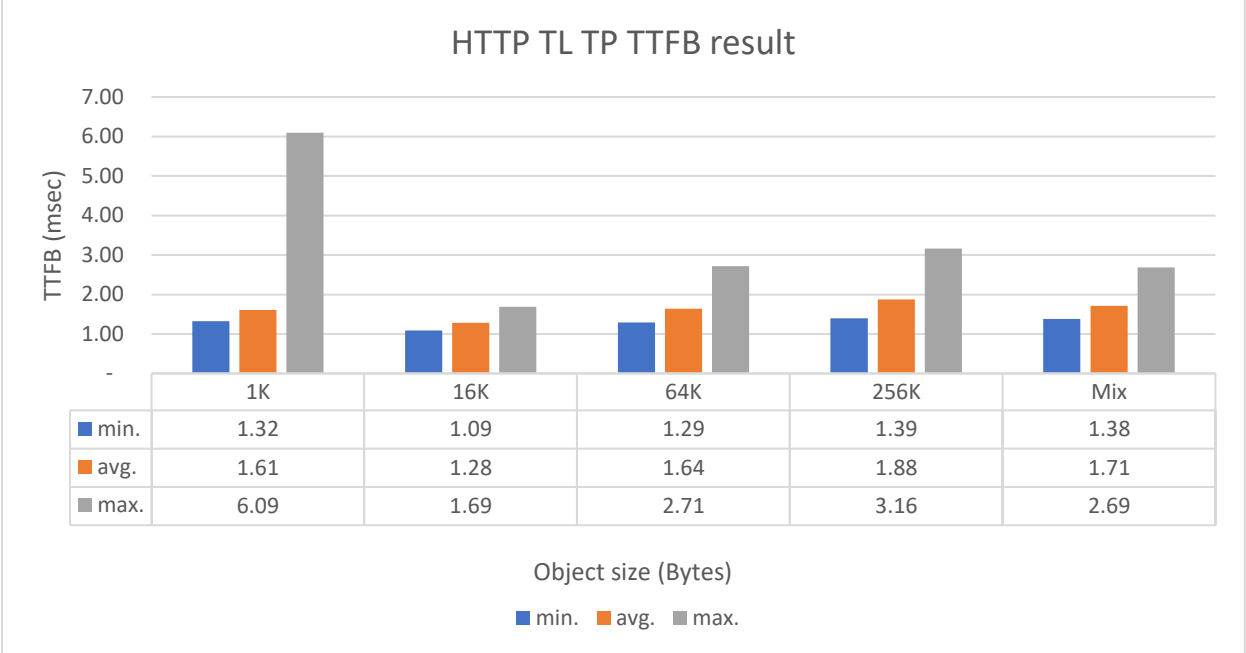
	1K	2K	4K	16K	64K
min.	1.64	1.72	1.83	2.36	3.74
avg.	1.75	1.83	1.96	2.52	3.98
max.	5.74	3.89	5.92	7.29	6.63

Figure 11 HTTPS TL CPS TTLB result



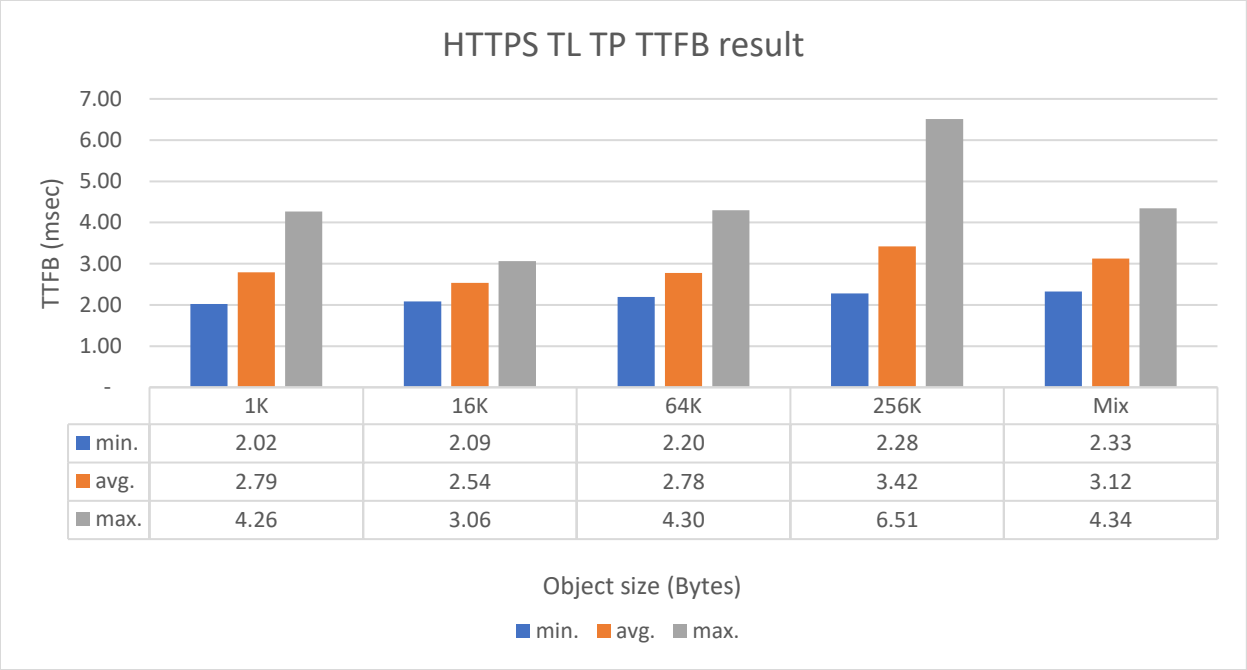
	1K	16K	64K	256K	Mix
HTTP TP (Mbits/s)	112	639	1,474	1,853	1,294
HTTPS TP (Mbits/s)	102	584	1,309	1,722	1,283
HTTP TPS	9,780	4,674	2,750	868	2,936
HTTPS TPS	7,608	4,171	2,427	804	2,892

Figure 12 TL Throughput result (TPS: Transaction Per Second)



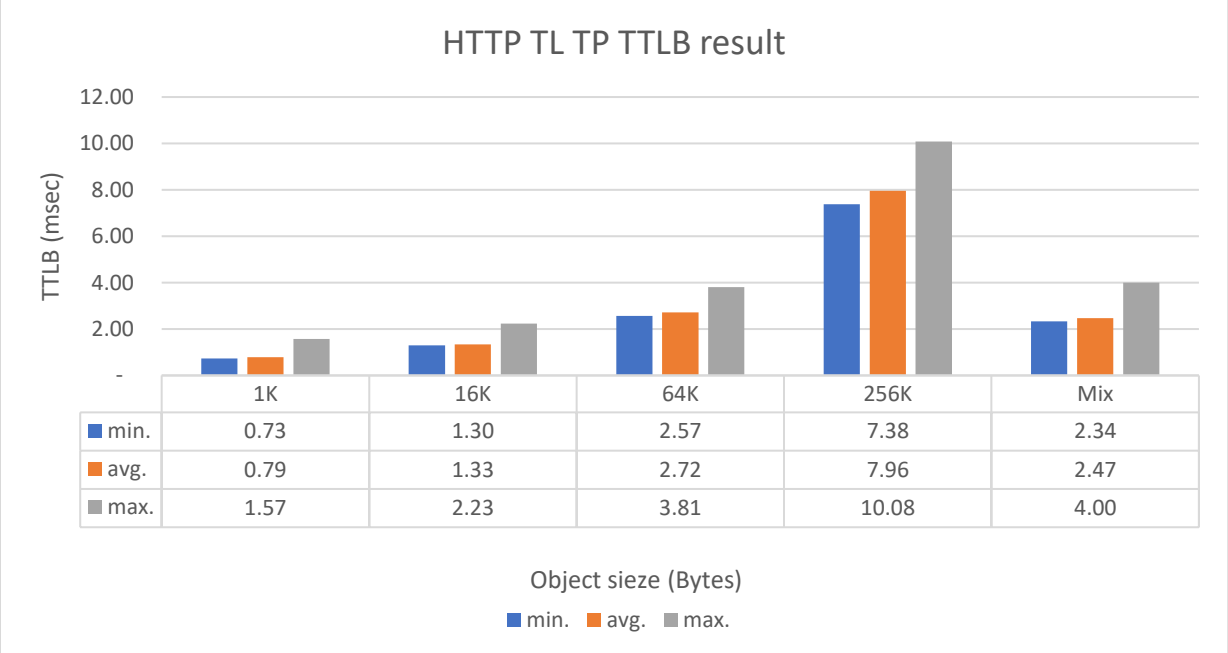
	1K	16K	64K	256K	Mix
min.	1.32	1.09	1.29	1.39	1.38
avg.	1.61	1.28	1.64	1.88	1.71
max.	6.09	1.69	2.71	3.16	2.69

Figure 13 HTTP TL TP TTFB result



	1K	16K	64K	256K	Mix
min.	2.02	2.09	2.20	2.28	2.33
avg.	2.79	2.54	2.78	3.42	3.12
max.	4.26	3.06	4.30	6.51	4.34

Figure 14 HTTPS TL TP TTFB result



	1K	16K	64K	256K	Mix
min.	0.73	1.30	2.57	7.38	2.34
avg.	0.79	1.33	2.72	7.96	2.47
max.	1.57	2.23	3.81	10.08	4.00

Figure 15 HTTP TL TP TTLB result

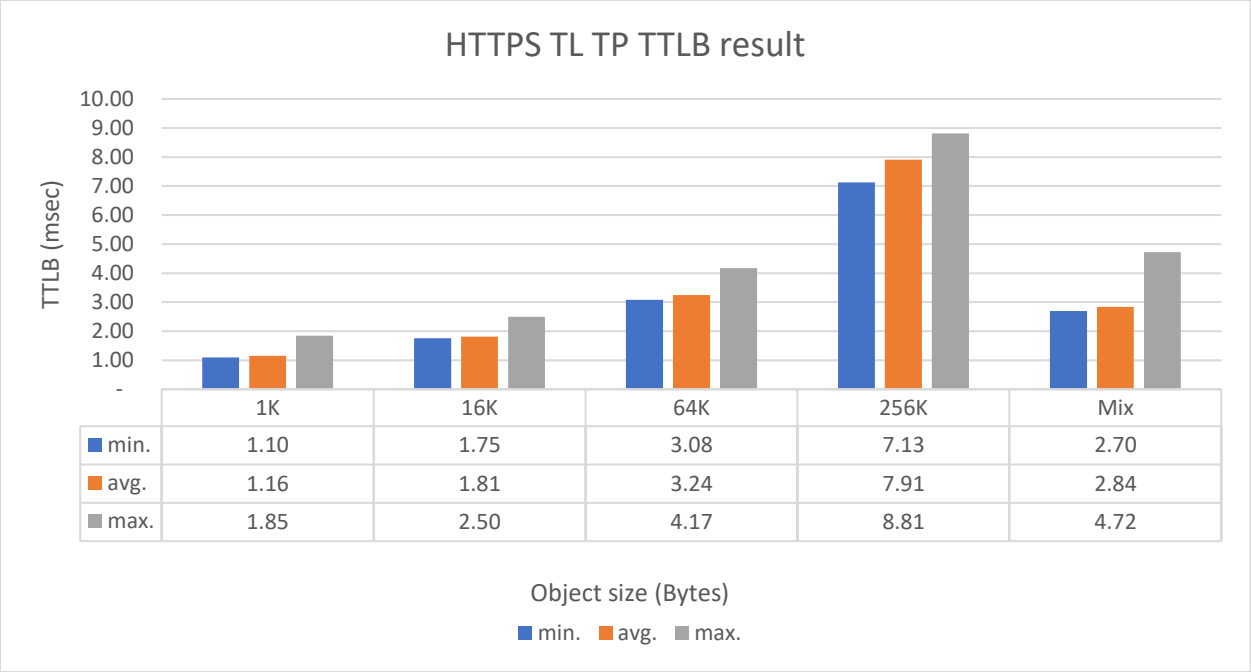
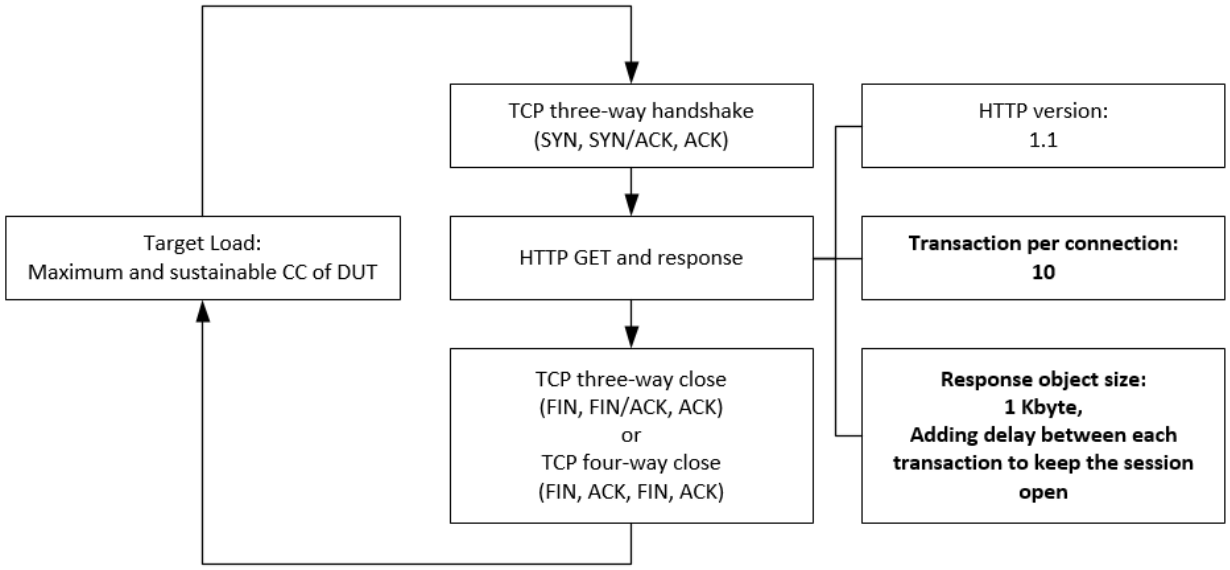


Figure 16 HTTPS TL TP TTLB result

Number	Test result validation criteria	Verdict
1	The number of failed application transactions (receiving any HTTP response code other than 200 OK) MUST be less than 0.001% (1 out of 100,000 transactions) of total attempted transactions.	Pass
2	The number of terminated TCP connections due to unexpected TCP RST sent by DUT/SUT MUST be less than 0.001% (1 out of 100,000 connections) of total initiated TCP connections.	Pass
3	During the sustain phase, traffic MUST be forwarded at a constant rate (considered as a constant rate if any deviation of traffic forwarding rate is less than 5%).	Pass
4	Concurrent TCP connections MUST be constant during steady state and any deviation of concurrent TCP connections MUST be less than 10%. This confirms the DUT opens and closes TCP connections at approximately the same rate.	Pass
5	After ramp up the DUT MUST achieve the "Target objective" defined in figure and remain in that state for the entire test duration (sustain phase).	Pass

Table 14. Test results validation criteria

3.5 Concurrent TCP/HTTP and HTTPS Connection Capacity (CC)



This test case is to measure the DUT's session table with HTTP and HTTPS sessions separately. The session table size is another critical parameter that customers need to consider. Therefore, we verified the DUT's session table size with a 1K object size. We configured 10 transactions per TCP connection and added a delay between each transaction so that the session could stay open during the whole sustain phase.

The stable concurrent TCP/HTTP connection during the sustain phase is 1,340,000.

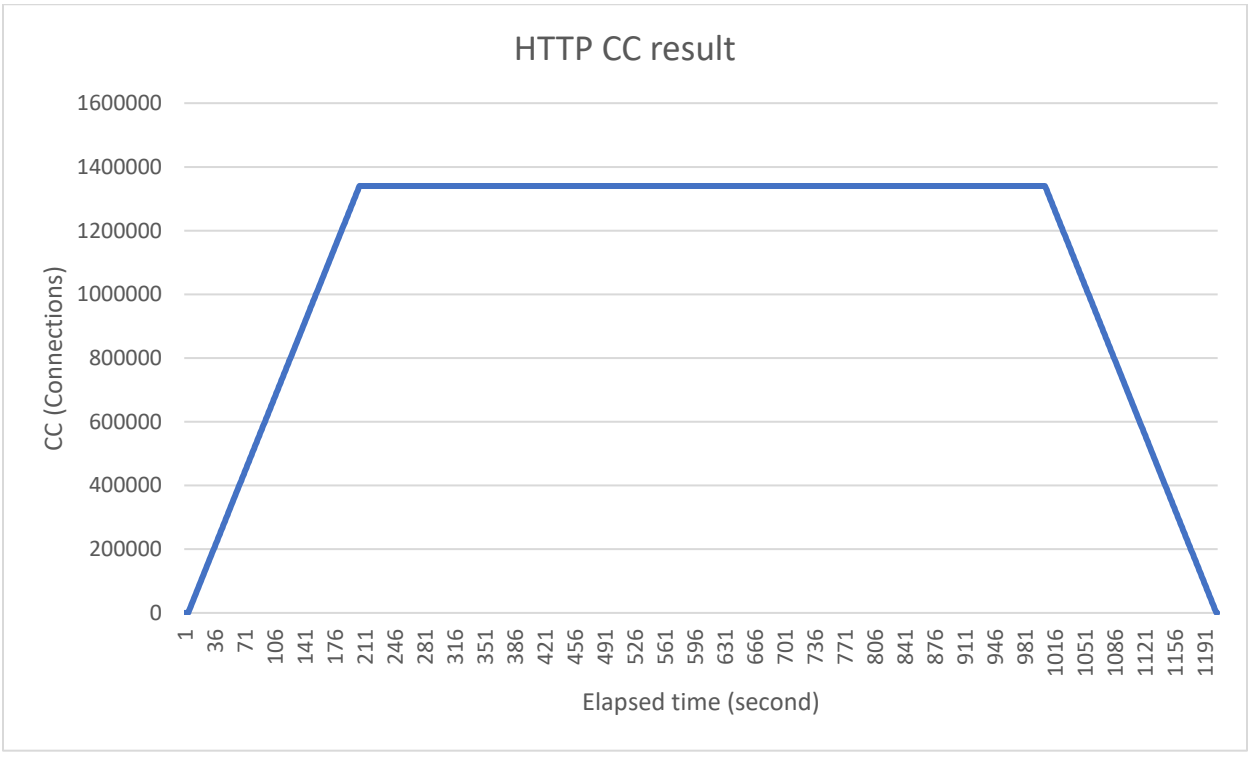


Figure 17 HTTP CC result

The stable concurrent HTTPS connection during the sustain phase is 657,000.

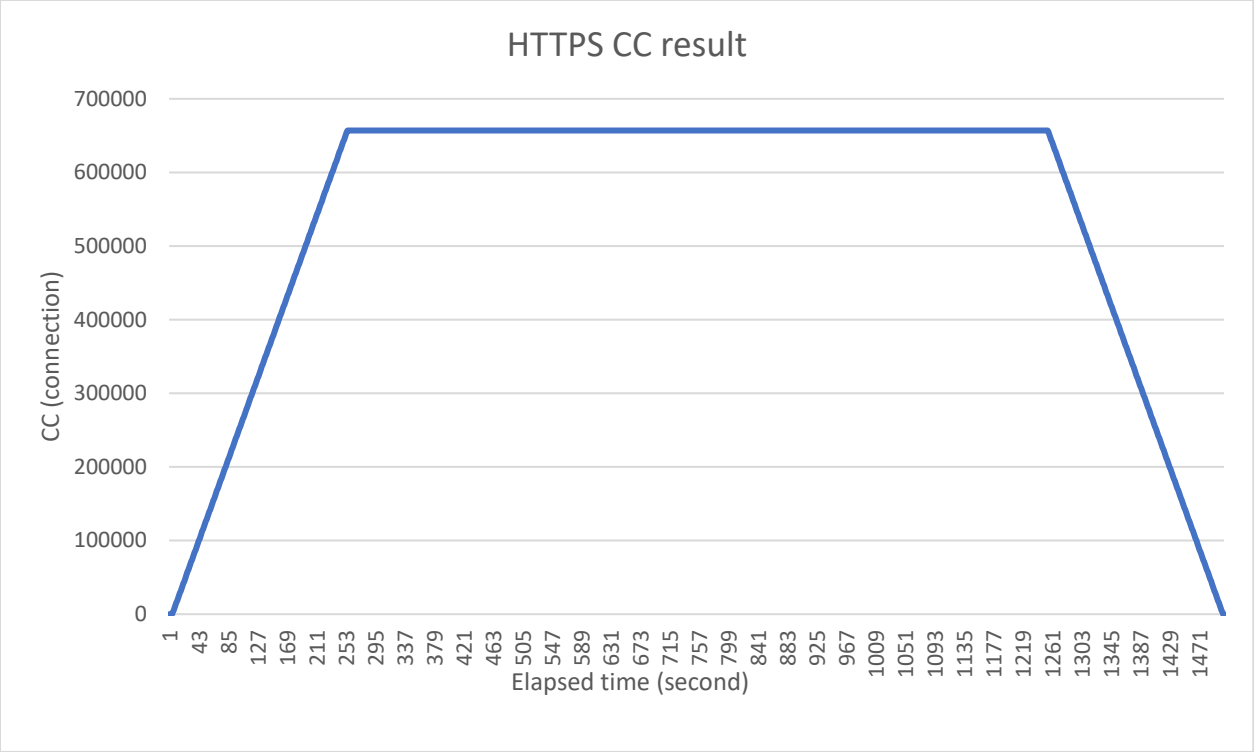


Figure 18 HTTPS CC result

Number	Test result validation criteria	Verdict
1	The number of failed application transactions (receiving any HTTP response code other than 200 OK) MUST be less than 0.001% (1 out of 100,000 transactions) of total attempted transactions.	Pass
2	The number of terminated TCP connections due to unexpected TCP RST sent by DUT/SUT MUST be less than 0.001% (1 out of 100,000 connections) of total initiated TCP connections.	Pass
3	During the sustain phase, traffic MUST be forwarded at a constant rate (considered as a constant rate if any deviation of traffic forwarding rate is less than 5%).	Pass

Table 15. Test results validation criteria

3.6 Security effectiveness test

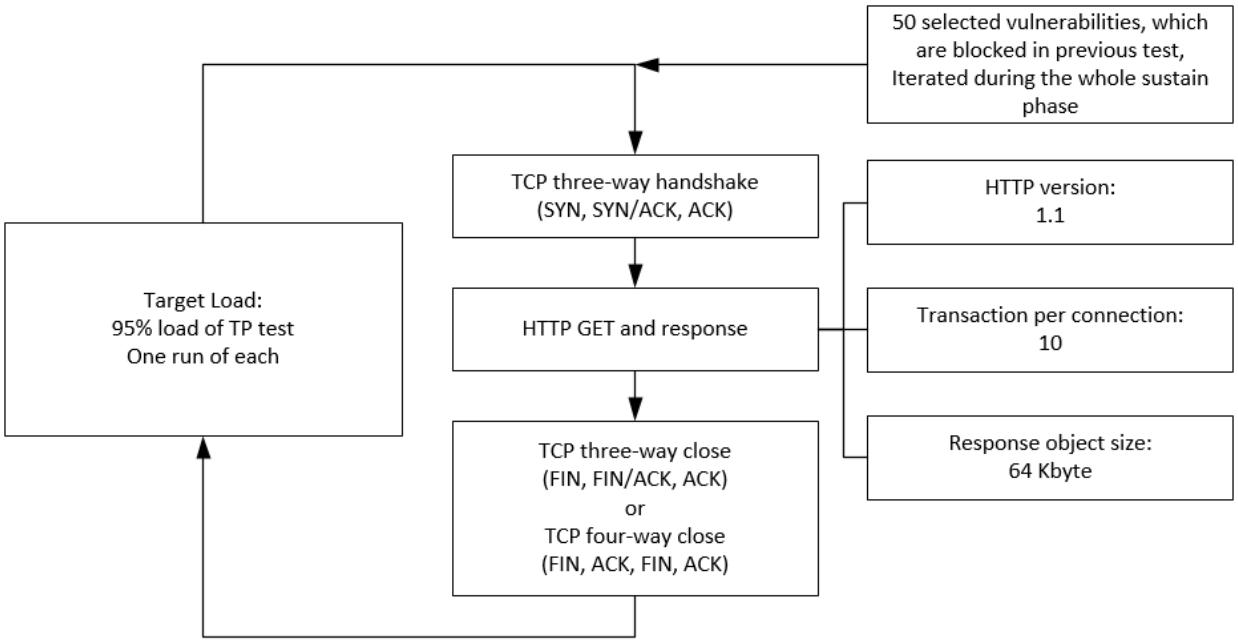
We sent malware, vulnerability, and evasion traffic to the DUT without any legitimate traffic to verify the security effectiveness of the DUT.

Attack category	Total attack	Public set block rate	Private set block rate
Malware	3809	3809/3809, 100%	N/A
Vulnerability	1381	1380/1381, 99.92%	180/180, 100%
Evasion	19	19/19, 100%[2]	N/A

Table 16. Test results validation criteria

2. Partially of the evasion attacks have been silently dropped by the DUT kernel, which means a RESET has been sent, but no relative logs are generated.

3.7 Security effectiveness under load



We selected 50 blocked vulnerabilities from the previous public set and sent them together with HTTP legitimate traffic. The 50 vulnerabilities were iterated during the whole sustain phase. The DUT needs to block all of them to pass the test. This test verifies that DUT's security engine can work properly under high load.

Load condition	Total attack	Iteration	Block rate	Verdict
95%	50	796	796/796, 100%	Pass

Table 17. Test results validation criteria