
University of New Hampshire
InterOperability
Laboratory
NetSecOPEN
TEST REPORT
NOVEMBER 2020
www.iol.unh.edu

MIKE DEICHMAN
WATCHGUARD TECHNOLOGIES INC.
MIKE.DEICHMAN@WATCHGUARD.COM

DEVICE AND TEST PLAN INFORMATION	
Device Under Test (DUT)	Firebox M5800
Test Specification/Suite	Benchmarking Methodology for Network Security Device Performance draft-ietf-bmwg-ngfw-performance-04
UNH-IOL Test Result ID	32703

CONTACT INFORMATION		
Testing Completed by	Hannah Dukeman	hdukeman@iol.unh.edu
Report Created by	Hannah Dukeman	hdukeman@iol.unh.edu
Report Reviewed by	Chris Brown	cbrown@iol.unh.edu

Please use Adobe Acrobat to validate the authenticity of this document.

TESTING NOTES

The following table contains any notes on the testing process or on general DUT behavior.

NOTES
Throughput performance with NetSecOPEN traffic mix portion of the methodology is currently still under development; therefore, not reported. Both public and private Common Vulnerabilities and Exposures (CVE) sets were tested against the device under test to confirm that the device exhibited the enabled security functionality. This portion of the methodology is currently still under development; therefore, the results are not officially reported for NetSecOPEN certification. The test tool is currently unable to send transactions after opening a TCP connection with the "HTTP Open Connections" template leveraged in test cases 7.5 & 7.9 Concurrent Connection Capacity. Therefore, the "HTTP Throughput" template was utilized.

REVISION HISTORY

The following table contains a revision history for this report.

REVISION	DATE	AUTHOR	EXPLANATION
1.0	11/13/2020	Hannah Dukeman	Initial version
2.0	11/30/2020	Chris Brown	Added an outline of the test setup and cipher suites used in the HTTPS test cases.

DEVICE INFORMATION

COMPONENT	DESCRIPTION
Device Name	Firebox M5800
UNH-IOL Device Identification Number	FW-WATCHGRD-0000027404
Device Model	M5800
Device Firmware	12.6.2 (Build 628008)
Interfaces Tested	Ethernet 8, Ethernet 9, Ethernet 10, Ethernet 11, Ethernet 16, Ethernet 17
Interfaces Speed	10G
Controller Name	N/A
Controller Model	N/A
Controller Firmware	N/A
Virtual VNF	N/A
VM Cores Used	N/A
VM RAM Used	N/A
Pinning Information	N/A
Hypervisor Name	N/A
Hypervisor Version	N/A

DEVICE ENABLED FEATURES

FEATURE	STATUS	
	ENABLED	DISABLED
SSL Inspection	✓	
IDS/IPS	✓	
Web Filtering		✓
Antivirus	✓	
Anti-Spyware	✓	
Anti-Botnet	✓	
DLP		✓
DDoS		✓
Certificate Validation		✓
Logging and Reporting	✓	
Application Identification	✓	

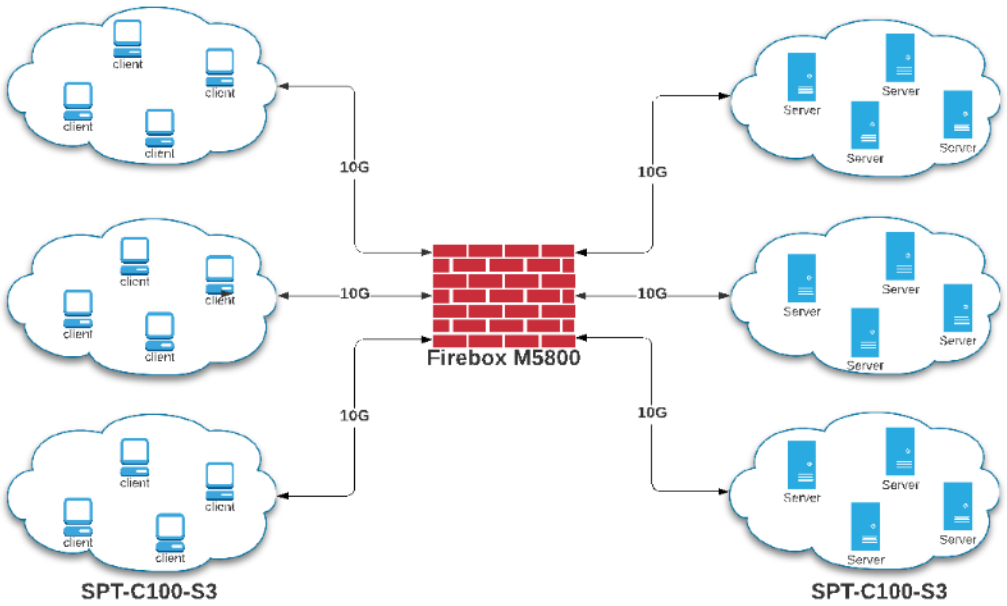
DEVICE ACL RULES

RULE TYPE	ACTION	# OF RULES
Application Layer	Block	20
Transport Layer	Block	100
IP Layer	Block	100
Application Layer	Allow	10
Transport Layer	Allow	3
IP Layer	Allow	3

TEST TOOL AND ENVIRONMENT INFORMATION

COMPONENT	DESCRIPTION	
Performance Test Equipment Vendor	Spirent	
Performance Hardware Name	SPT-C100-S3	
Performance Hardware Firmware	5.13.0817	
Performance Hardware Interface Type	10G	
Performance Application Software Name	Cyberflood	
Performance Application Software Version	20.5.4008	
Efficiency Test Equipment Vendor	Spirent	
Efficiency Hardware Name	SPT-C100-S3	
Efficiency Hardware Firmware	5.13.0817	
Efficiency Hardware Interface Type	10G	
Efficiency Application Software Name	Cyberflood	
Efficiency Application Software Version	20.5.4008	
Client IP Subnet 1	10.10.0.0/21	
Client IP Subnet 2	10.12.0.0/21	
Client IP Subnet 3	10.14.0.0/21	
Server IP Subnet 1	10.11.0.0/21	
Server IP Subnet 2	10.13.0.0/21	
Server IP Subnet 3	10.15.0.0/21	
Traffic Distribution Ratio	**IPv4**	**IPv6**
	100%	0%
Cipher Suite	ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048	

TESTBED SETUP



KPI RESULT SUMMARY

SECTION 7.1

TEST CASE	KPI	TRAFFIC MIX (SSL DISABLED)	TRAFFIC MIX (SSL ENABLED)
Throughput Performance with NetSecOPEN Traffic Mix	Throughput	N/A	N/A
	TPS	N/A	N/A
	TTFB	N/A	N/A
	TTLB	N/A	N/A

SECTION 7.2

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTP Connections Per Second	CPS	19,766	19,358	19,020	17,536	13,409

SECTION 7.3

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTP Throughput	TPUT (Kbit/s)	343,594	3,291,631	10,242,651	15,751,473	8,750,612
	TPS	27,532	24,061	19,071	7,363	19,807

SECTION 7.4

TEST CASE	KPI	CPS 1K	CPS 16K	CPS 64K	TPUT 1K	TPUT 16K	TPUT 64K
TCP/HTTP Transaction Latency	TTFB Average (msec)	1.0	1.2	1.4	0.7	0.9	1.3
	TTFB Minimum (msec)	0.438	0.444	0.439	0.395	0.415	0.431
	TTFB Maximum (msec)	74.946	55.607	59.98	49.543	48.913	66.999
	TTLB Average (msec)	1.57	1.85	2.73	200.63	1.08	2.04
	TTLB Minimum (msec)	0.441	0.719	1.325	0.755	0.521	0.916
	TTLB Maximum (msec)	60.862	57.312	206.094	256.54	77.444	207.52

SECTION 7.5

TEST CASE	KPI	1K
Concurrent TCP/HTTP Connection Capacity	CC	119,997

SECTION 7.6

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTPS Connections Per Second	CPS	1,653	1,641	1,632	1,602	1,519

SECTION 7.7

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTPS Throughput	TPUT (Kbit/s)	208,401	1,512,966	3,600,194	5,002,736	3,121,531
	TPS	13,284	10,805	6,654	2,332	6,999

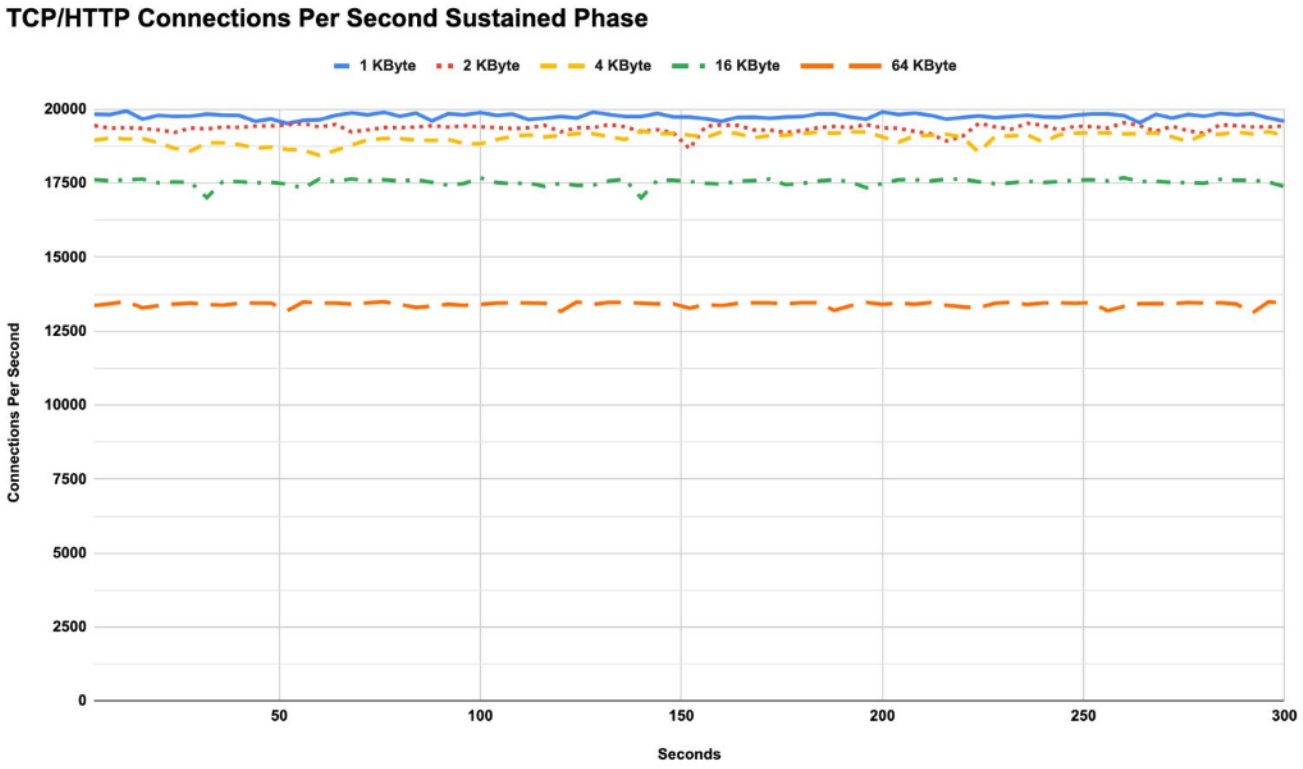
SECTION 7.8

TEST CASE	KPI	CPS 1K	CPS 16K	CPS 64K	TPUT 1K	TPUT 16K	TPUT 64K
TCP/HTTPS Transaction Latency	TTFB Average (msec)	10.7	10.8	10.2	10.7	9.9	9.8
	TTFB Minimum (msec)	5.22	7.017	4.888	7.099	7.071	7.082
	TTFB Maximum (msec)	77.19	72.972	68.701	70.42	83.599	123.612
	TTLB Average (msec)	196.41	196.98	210.44	221.33	21.35	29.90
	TTLB Minimum (msec)	0.772	142.333	4.141	200.46	0.806	1.832
	TTLB Maximum (msec)	249.754	249.752	1533.709	451.033	248.626	1117.116

SECTION 7.9

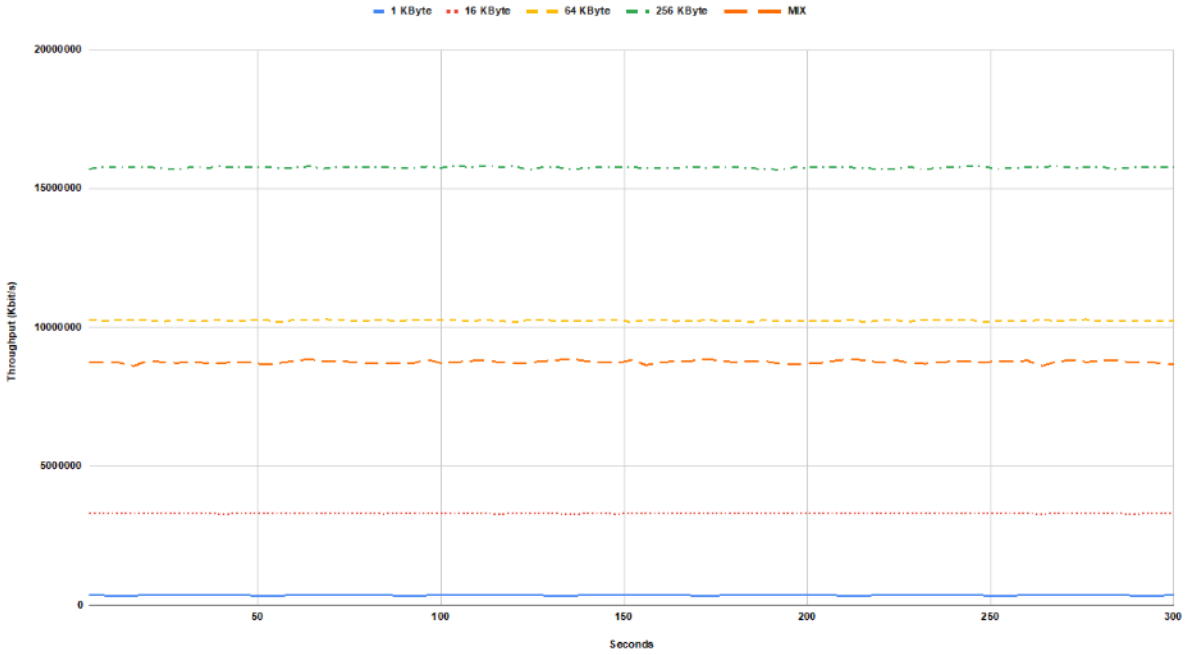
TEST CASE	KPI	1K
Concurrent TCP/HTTPS Connection Capacity	CC	149,994

GRAPHS

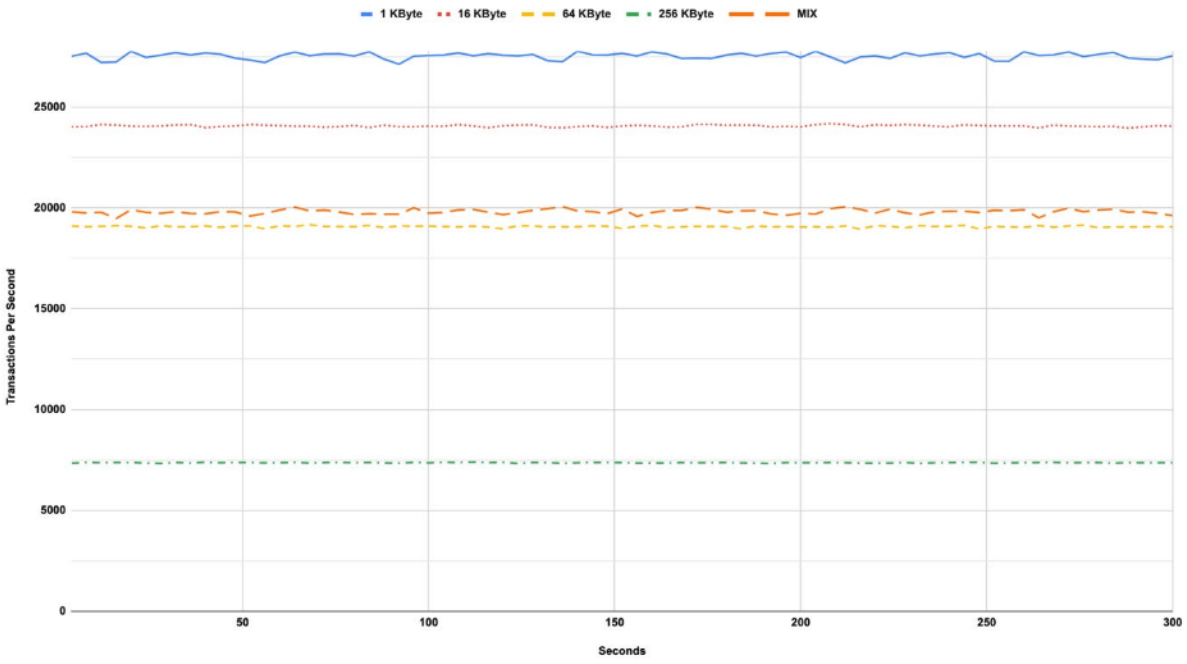


Maximum sustainable TCP/HTTP connection establishment rate supported by the DUT under different throughput load conditions.

HTTP Throughput Sustained Phase

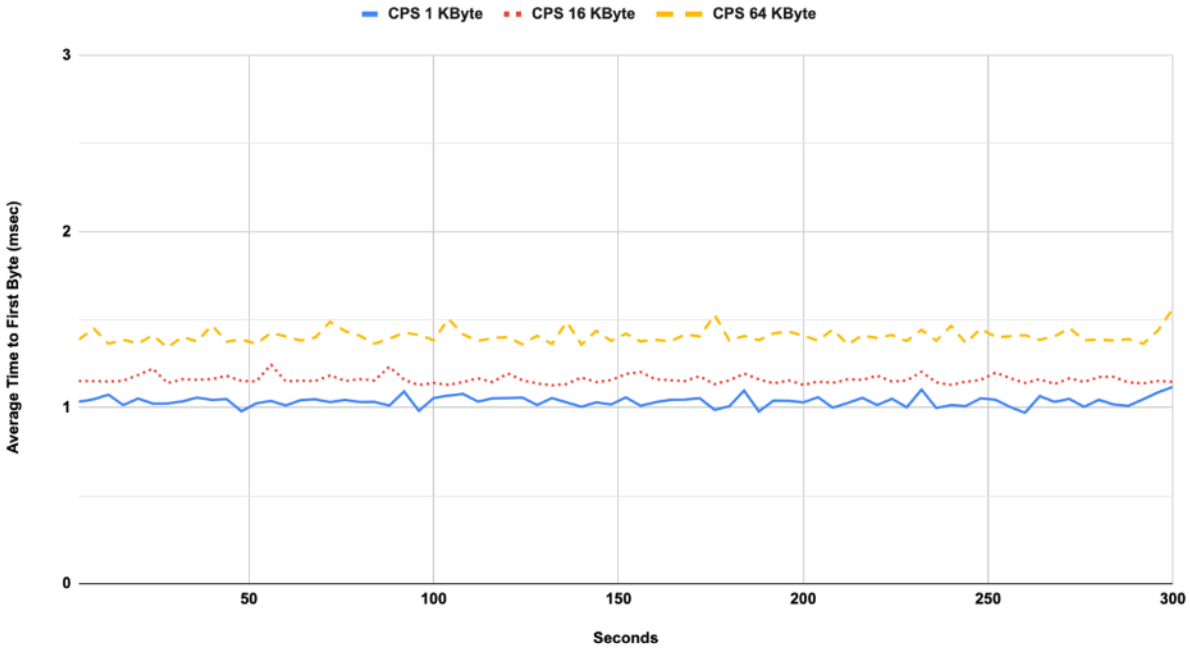


HTTP Transactions Per Second Sustained Phase

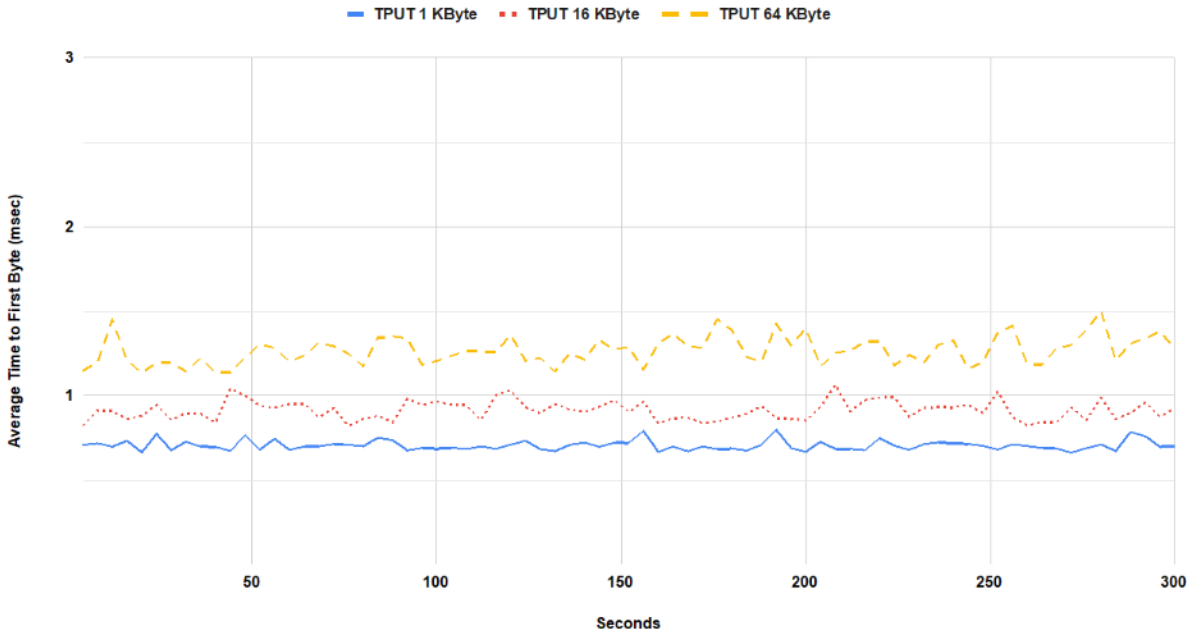


Maximum sustainable throughput for HTTP transactions varying the HTTP response object size.

TCP/HTTP Transaction Latency Connections Per Second Sustained Phase

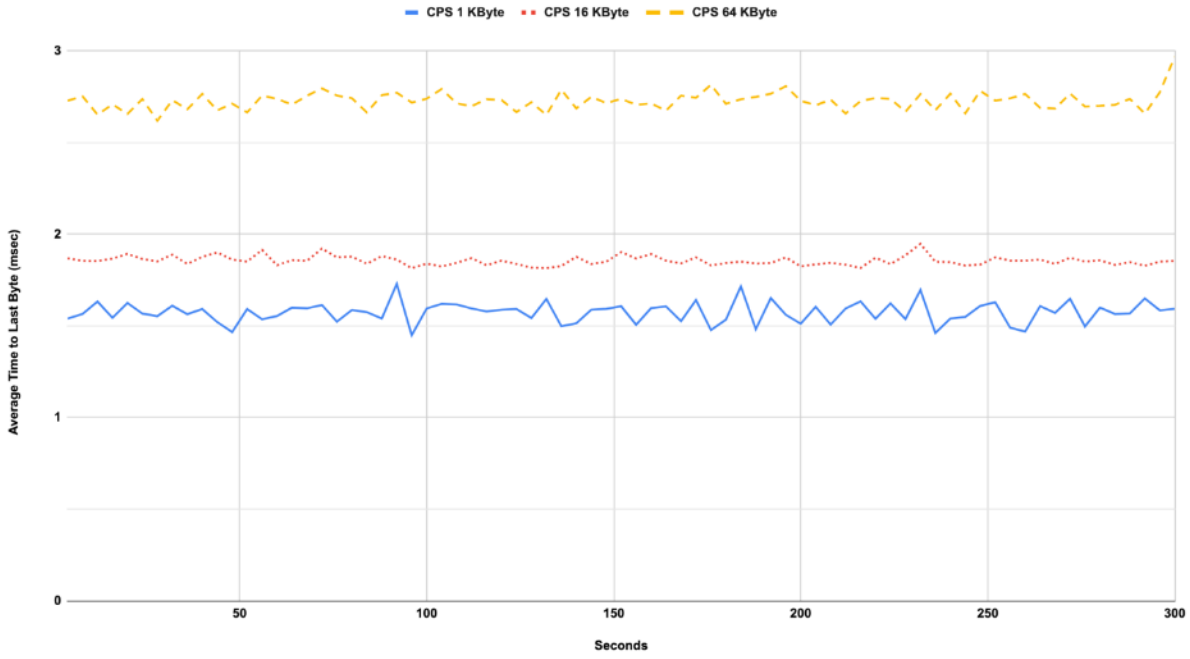


TCP/HTTP Transaction Latency Throughput Sustained Phase

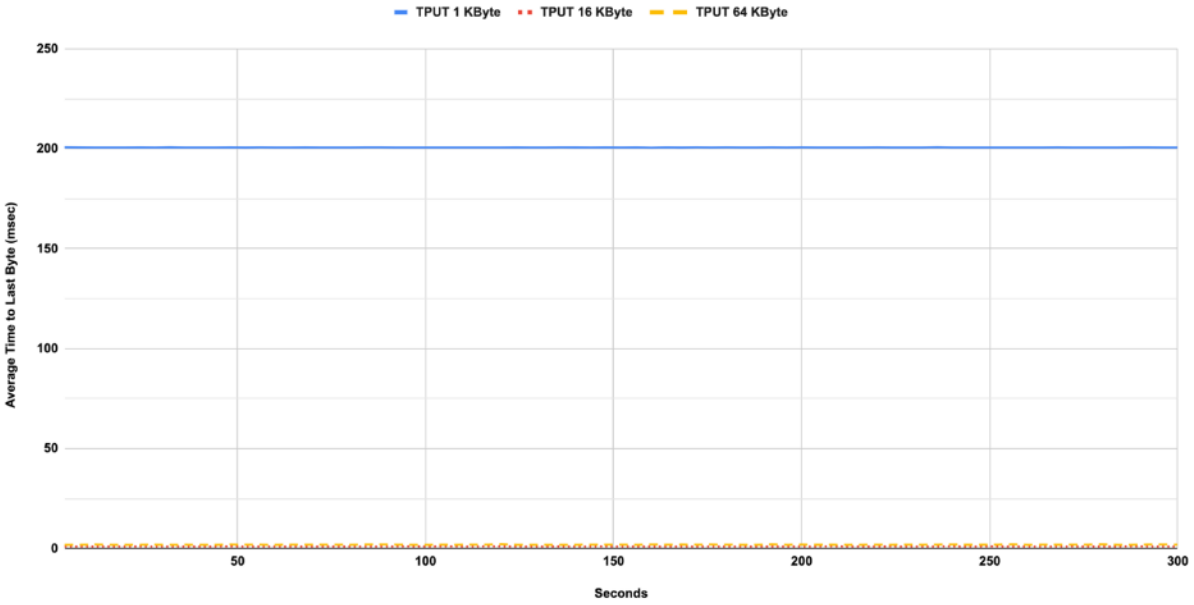


Average HTTP transaction latency time to first byte with sustainable HTTP transactions per second under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

TCP/HTTP Transaction Latency Connections Per Second Sustained Phase

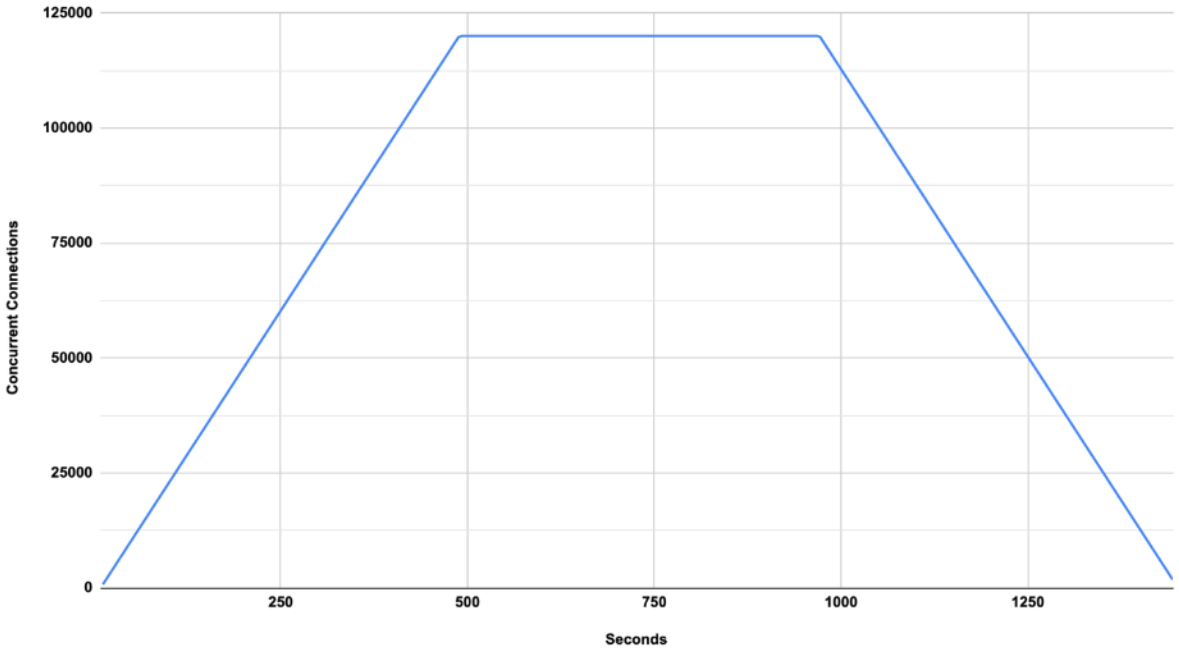


TCP/HTTP Transaction Latency Throughput Sustained Phase



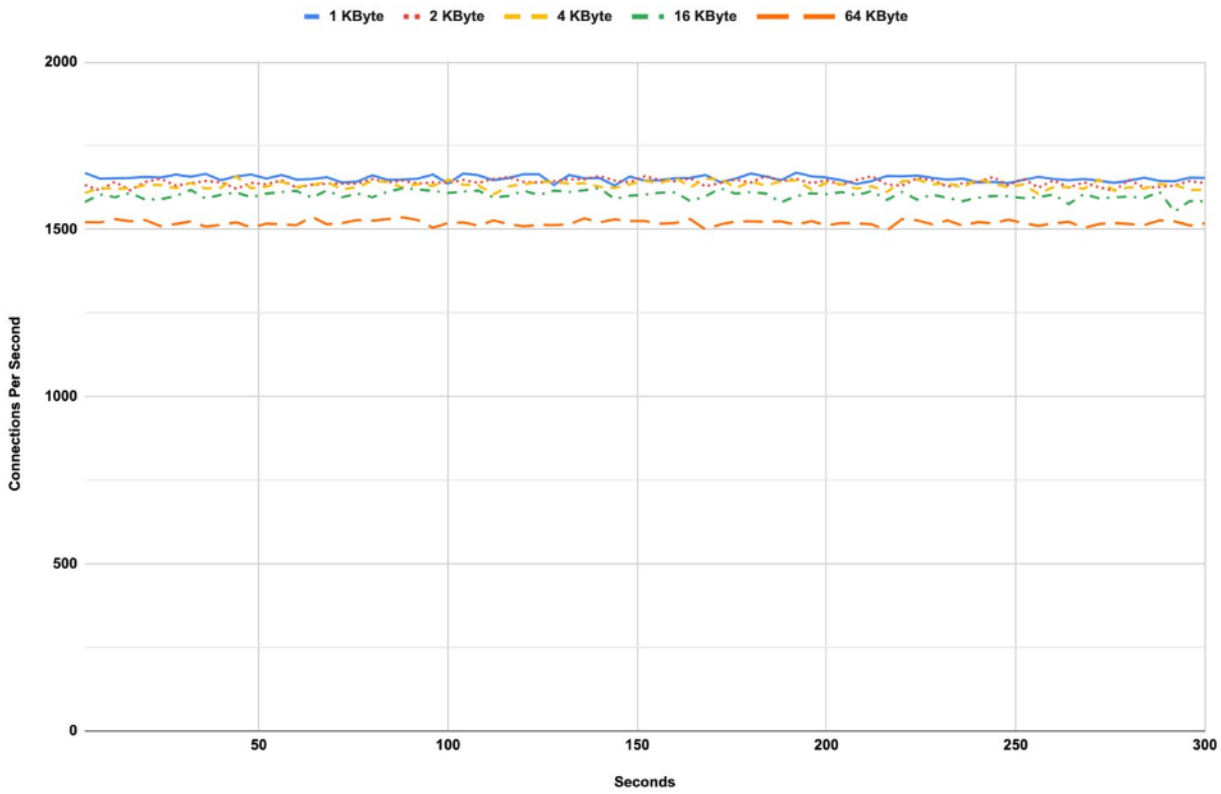
Average HTTP transaction latency time to last byte with sustainable HTTP transactions per second under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

Concurrent TCP/HTTP Connection Capacity



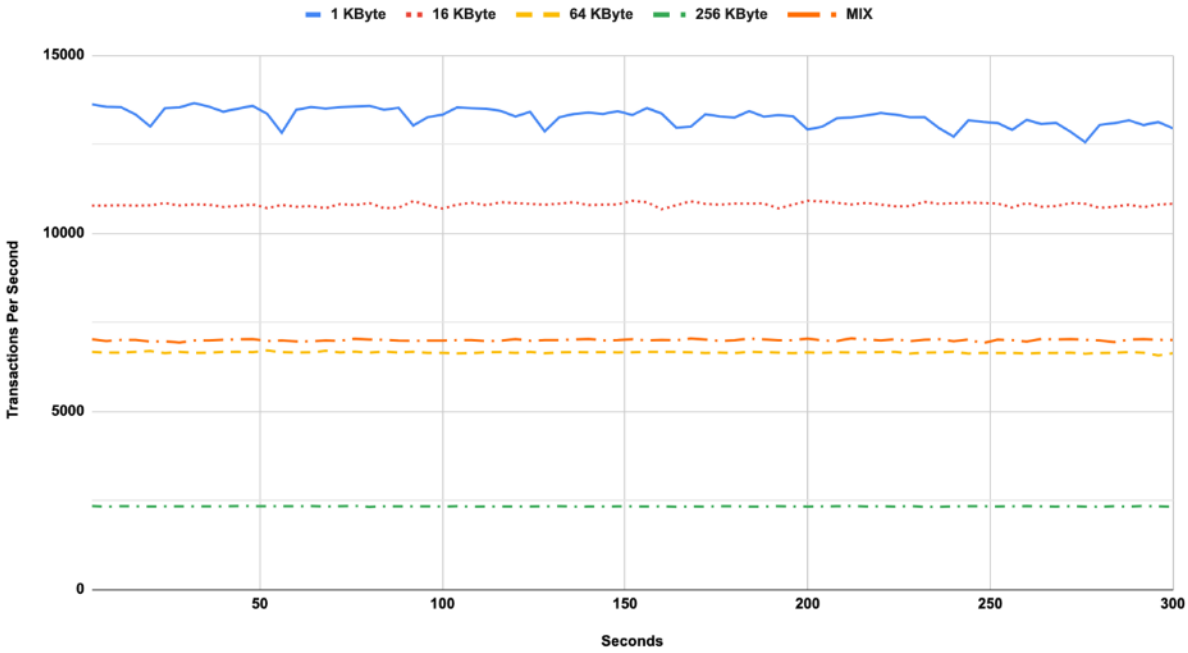
Maximum achievable HTTP connections per second with 1 KByte object size.

TCP/HTTPS Connections Per Second Sustained Phase

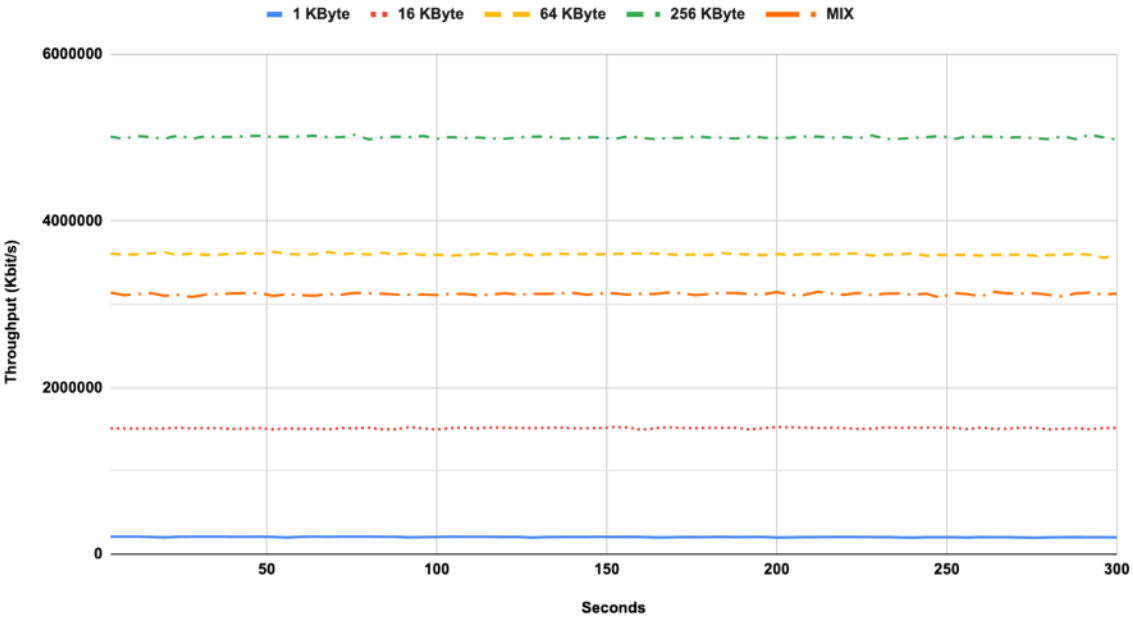


Maximum sustainable TCP/HTTPS connection establishment rate supported by the DUT under different throughput load conditions.

HTTPS Transactions Per Second Sustained Phase

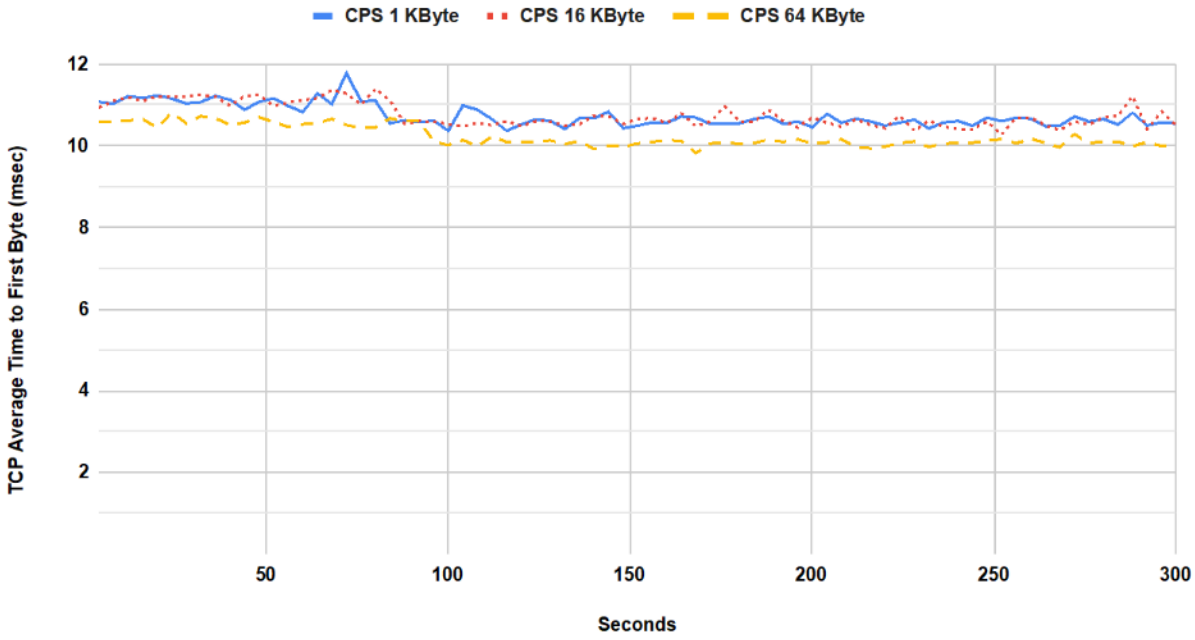


HTTPS Throughput Sustained Phase

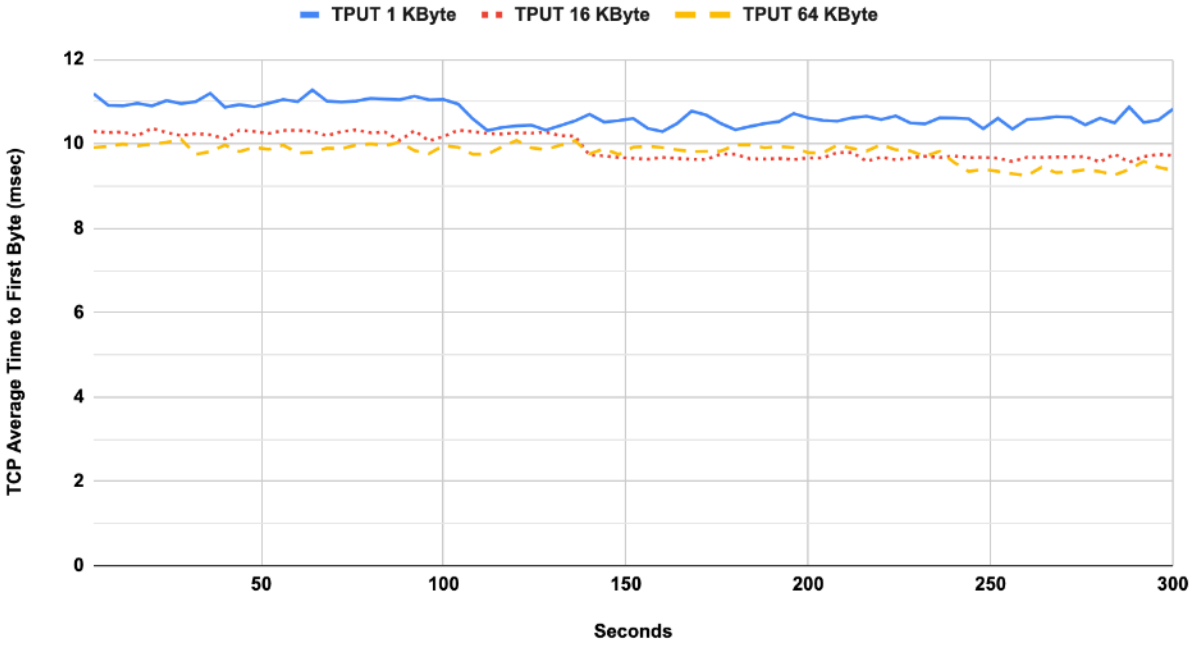


Maximum sustainable throughput for HTTPS transactions varying the HTTPS response object size.

TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase

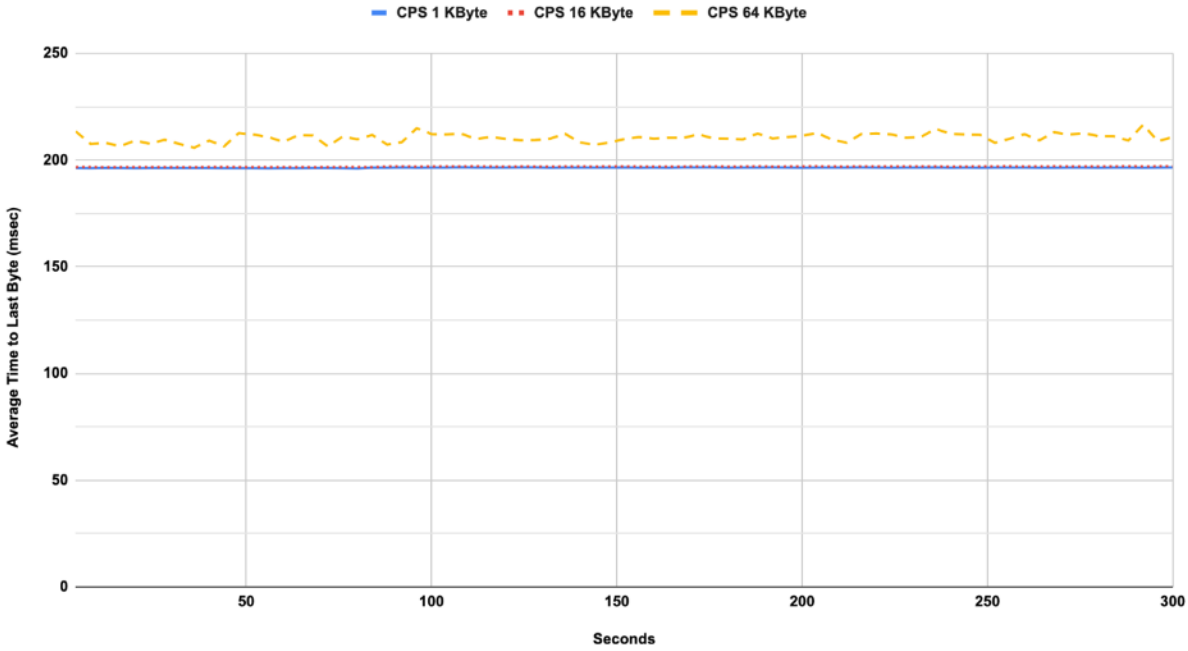


TCP/HTTPS Transaction Latency Throughput Sustained Phase

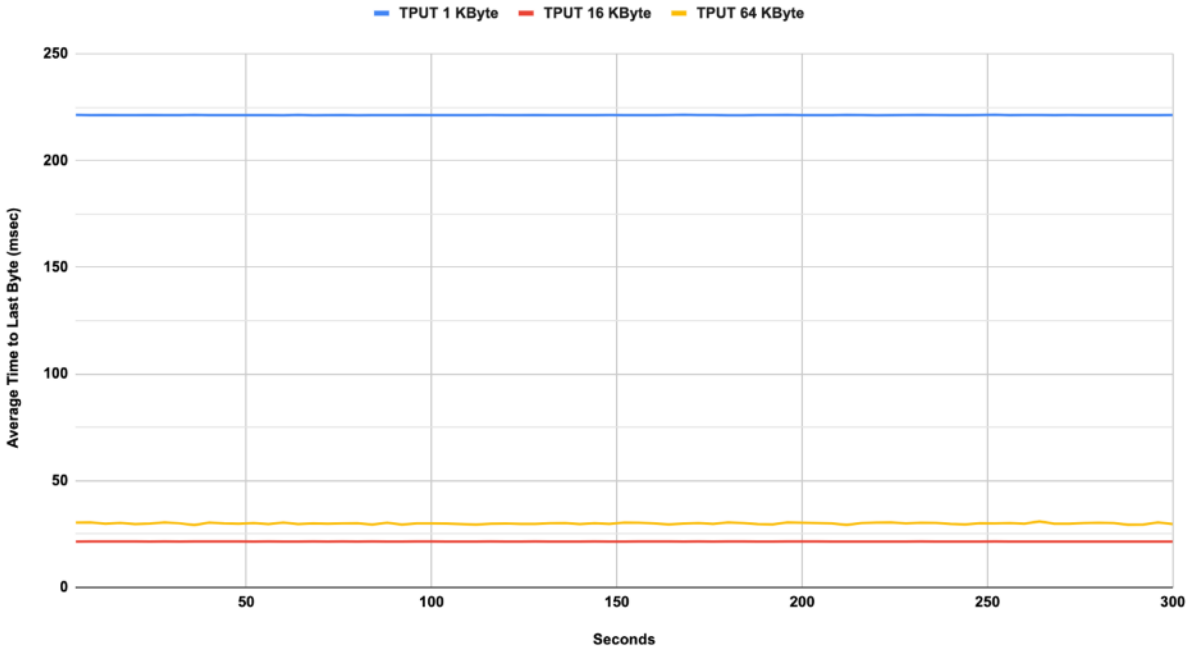


Average HTTPS transaction latency time to first byte with sustainable HTTPS transactions per second under different HTTPS response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase

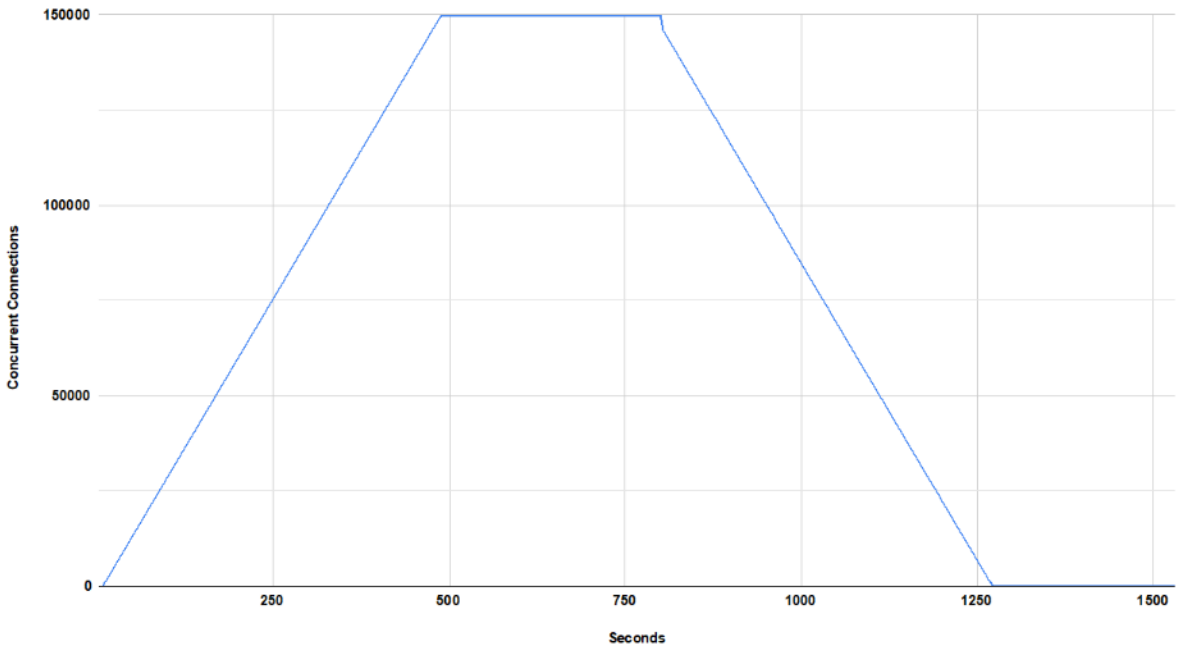


TCP/HTTPS Transaction Latency Throughput Sustained Phase



Average HTTPS transaction latency time to last byte with sustainable HTTPS transactions per second under different HTTPS response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

Concurrent TCP/HTTPS Connection Capacity



Maximum achievable HTTPS connections per second with 1 KByte object size.

APPENDICES

APPENDIX 1: KPI KEY

The following table contains possible KPIs and their meanings.

KPI	MEANING	INTERPRETATION
CPS	TCP Connections Per Second	Measures the average established TCP connections per second in the sustaining period. For "TCP/HTTP(S) Connection Per Second" benchmarking test scenario, the KPI is measured average established and terminated TCP connections per second simultaneously.
TPUT	Throughput	Measures the average Layer 2 throughput within the sustaining period as well as average packets per seconds within the same period. The value of throughput is expressed in Kbit/s.
TPS	Application Transactions Per Second	Measures the average successfully completed application transactions per second in the sustaining period.
TTFB	Time to First Byte	Measure the minimum, maximum and average time to first byte. TTFB is the elapsed time between sending the SYN packet from the client and receiving the first byte of application date from the DUT/SUT. TTFB SHOULD be expressed in milliseconds.
TTLB	Time to Last Byte	Measures the minimum, maximum and average per URL response time in the sustaining period. The latency is measured at Client and in this case would be the time duration between sending a GET request from Client and the receival of the complete response from the server. TTLB is expressed in milliseconds.
CC	Concurrent TCP Connections	Measures the average concurrent open TCP connections in the sustaining period.
N/A	Not Applicable	This test does not apply to the device type or is not applicable to the testing program selected.

APPENDIX 2: CVE DETECTION RATES

As stated previously, we performed the CVE check to verify the security functionality of the DUT during 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:

PREVENT SCENARIO	SCENARIOS TOTAL	BLOCKED	NOT BLOCKED
Public CVE	435	96% (419)	4% (16)
Private CVE	33	94% (31)	6% (2)