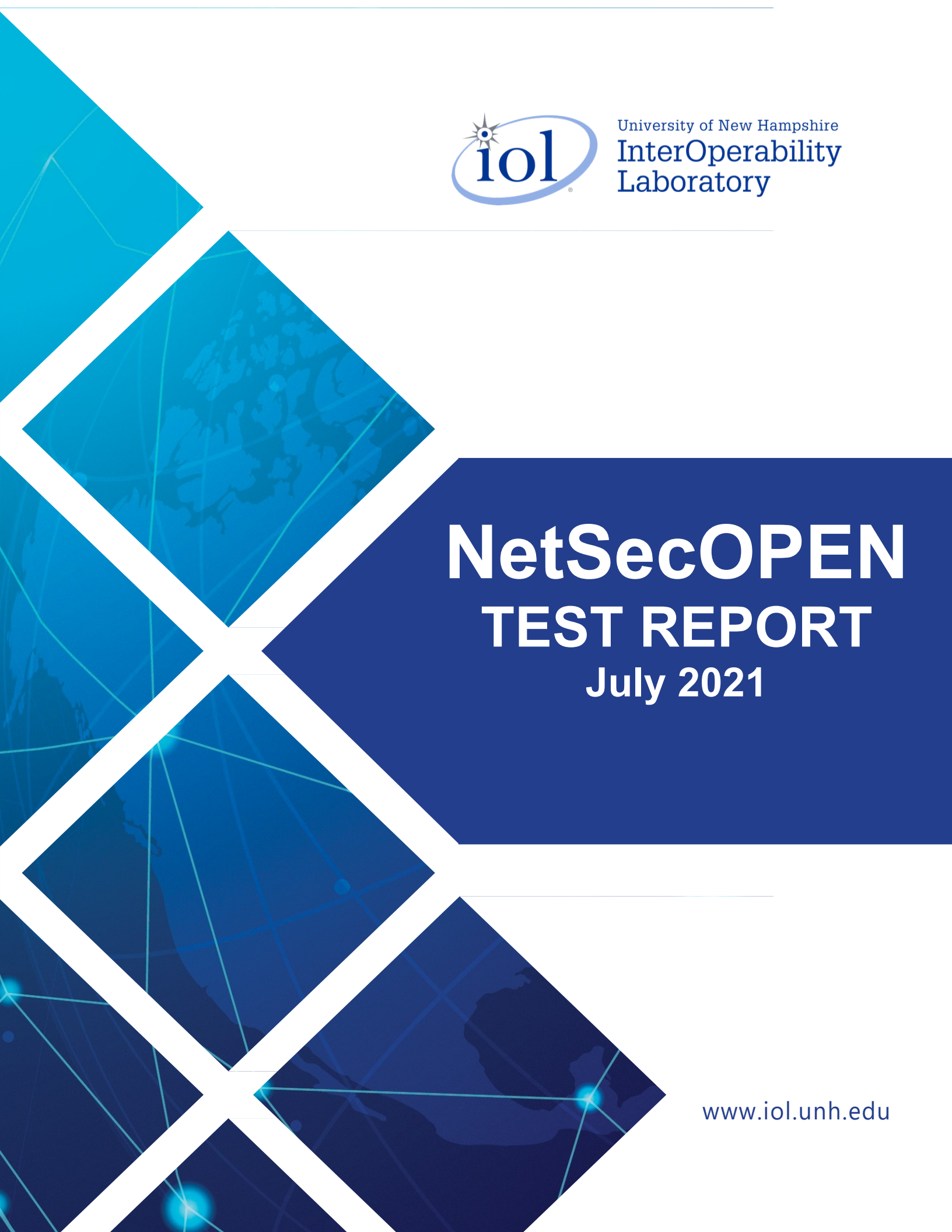


NetSecOPEN
TEST REPORT
July 2021

www.iol.unh.edu

DAN CARTMILL
TREND MICRO INC.
DAN_CARTMILL@TRENDMICRO.COM

DEVICE AND TEST PLAN INFORMATION	
Device Under Test (DUT)	TippingPoint 5500TX
Test Specification/Suite	Benchmarking Methodology for Network Security Device Performance draft-ietf-bmwg-ngfw-performance-08
UNH-IOL Test Result ID	33071

CONTACT INFORMATION		
Testing Completed by	Chris Brown	cbrown@iol.unh.edu
Report Created by	Chris Brown	cbrown@iol.unh.edu
Report Reviewed by	Timothy Carlin	tjcarlin@iol.unh.edu

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

Digitally signed by Timothy Carlin
Date: 2021.08.03 14:36:04 -04'00'

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. Sections 7.5 and 7.9 Concurrent Connection Capacity test cases were executed using BreakingPoint application (9.10.110.81). It was observed that the device under test would go into Intrinsic HA Fallback mode during the TCP/HTTPS Connections Per Second test case (Section 7.6); therefore, hardware acceleration was disabled on the device under test for all test cases to prevent it from going into fallback mode.

REVISION HISTORY

The following table contains a revision history for this report.

REVISION	DATE	AUTHOR	EXPLANATION
1.0	07/07/2021	Chris Brown	Initial version
2.0	02/08/2021	Chris Brown	Adjusted column headers in section 7.6 with correct object sizes

DEVICE INFORMATION

COMPONENT	DESCRIPTION
Device Name	TippingPoint 5500TX
UNH-IOL Device Identification Number	FW-TRENDMIC-0000027415
Device Model	5500TX
Device Firmware	5.4.1.1649
Interfaces Tested	Slot 1 Segment 1 Port A, Slot 1 Segment 1 Port B, Slot 1 Segment 2 Port A, Slot 1 Segment 2 Port B
Interfaces Speed	10G
Controller Name	TippingPoint Security Management System
Controller Model	Security Management System
Controller Firmware	5.4.0.204385
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	✓	
Anti-Malware	✓	
Anti-Spyware	✓	
Anti-Botnet	✓	
Logging and Reporting	✓	
Application Identification	✓	
Deep Packet Inspection	✓	
Anti-Evasion	✓	

DEVICE ACL RULES

RULE TYPE	ACTION	NUMBER OF RULES
Application Layer	Block	10
Transport Layer	Block	50
IP Layer	Block	50
Application Layer	Allow	10
Transport Layer	Allow	2
IP Layer	Allow	2

TEST TOOL AND ENVIRONMENT INFORMATION

COMPONENT	DESCRIPTION	
Performance Test Equipment Vendor	Ixia	
Performance Hardware Name	PerfectStorm One	
Performance Hardware Firmware	9.10.2000.24	
Performance Hardware Interface Type	10G	
Performance Application Software Name	BreakingPoint QuickTest NetSecOPEN LITE	
Performance Application Software Version	9.10.104.22	
Security Effectiveness Test Equipment Vendor	Spirent	
Security Effectiveness Hardware Name	SPT-C100-S3	
Security Effectiveness Hardware Firmware	5.18.0309	
Security Effectiveness Hardware Interface Type	10G	
Security Effectiveness Application Software Name	Cyberflood	
Security Effectiveness Application Software Version	21.1.4286	
Client IP Subnet 1	10.10.0.0/21	
Client IP Subnet 2	10.12.0.0/21	
Server IP Subnet 1	10.11.0.0/21	
Server IP Subnet 2	10.13.0.0/21	
Traffic Distribution Ratio	**IPv4**	**IPv6**
	100%	0%
Cipher Suite	ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048	

TESTBED SETUP

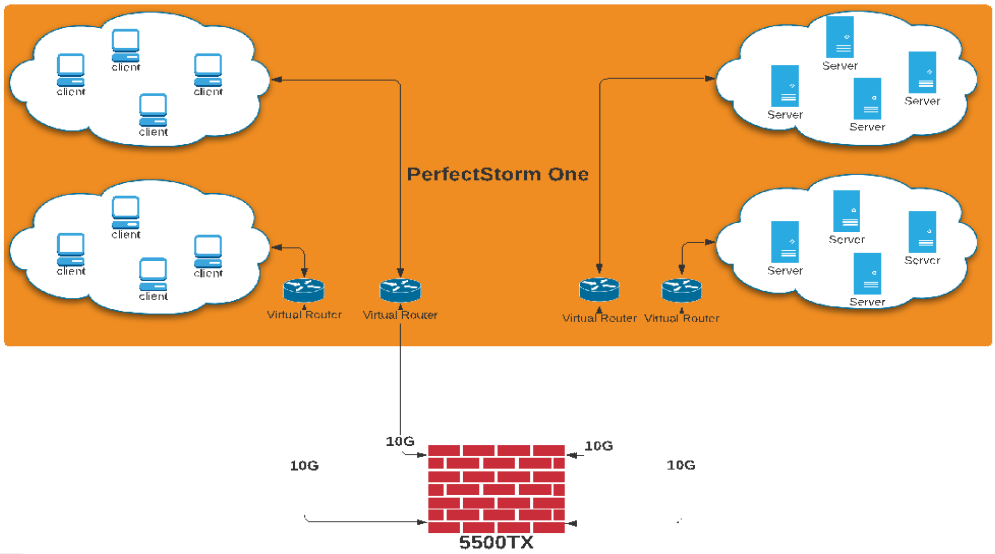


Figure 1: Topology with Performance Test Equipment Vendor

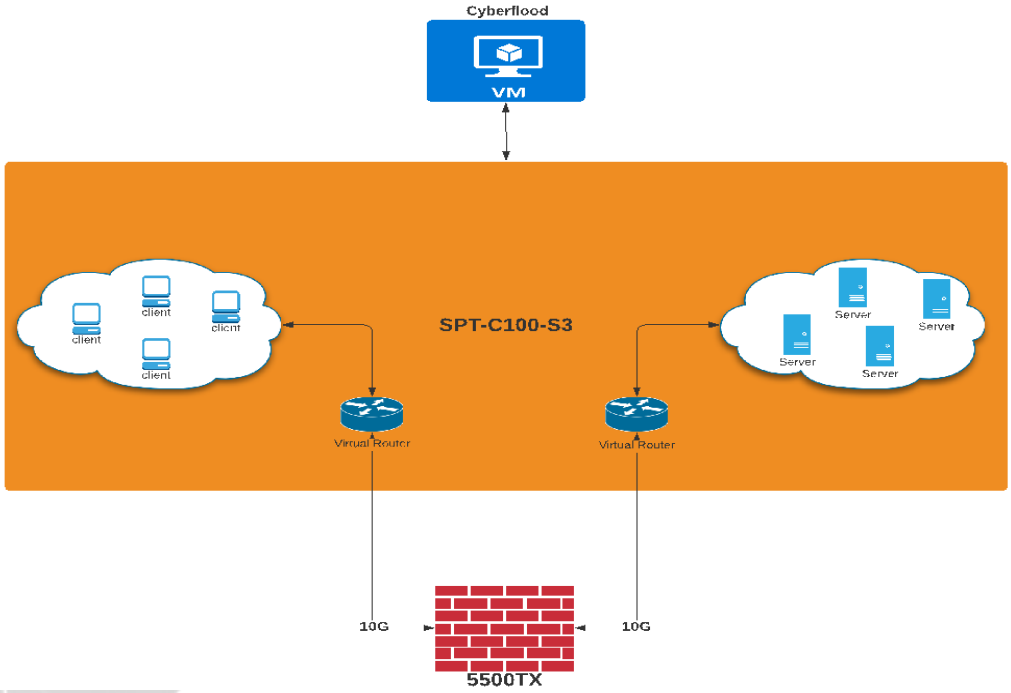


Figure 2: Topology with Security Effectiveness Test Equipment Vendor

KPI RESULT SUMMARY

SECTION 7.2

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTP Connections Per Second	CPS	137,962	127,671	118,987	55,030	16,444

SECTION 7.3

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTP Throughput	TPUT (Mbps)	5,471	8,638	9,829	9,967	9,750
	TPS	467,570	61,865	17,933	4,535	21,614

SECTION 7.4

TEST CASE	KPI	CPS 1K	CPS 16K	CPS 64K	TPUT 1K	TPUT 16K	TPUT 64K
HTTP Transaction Latency	TTFB Average (msec)	0.14	0.20	0.26	0.15	0.25	0.76
	TTFB Minimum (msec)	0	0	0	0	0	0
	TTFB Maximum (msec)	20	20	19	26	22	22
	TTLB Average (msec)	0.15	0.41	1.12	0.15	0.45	1.68
	TTLB Minimum (msec)	0	0	0	0	0	0
	TTLB Maximum (msec)	20	23	27	26	24	24

SECTION 7.5

TEST CASE	KPI	1K
Concurrent TCP/HTTP Connection Capacity	CC	14,000,000

SECTION 7.6

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTPS Connections Per Second	CPS	2,383	2,371	2,355	2,259	2,018
	HR	1K				
		2,383				

SECTION 7.7

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTPS Throughput	TPUT (Mbps)	268	2,085	4,530	6,682	4,319
	TPS	19,538	14,704	8,176	3,052	9,516

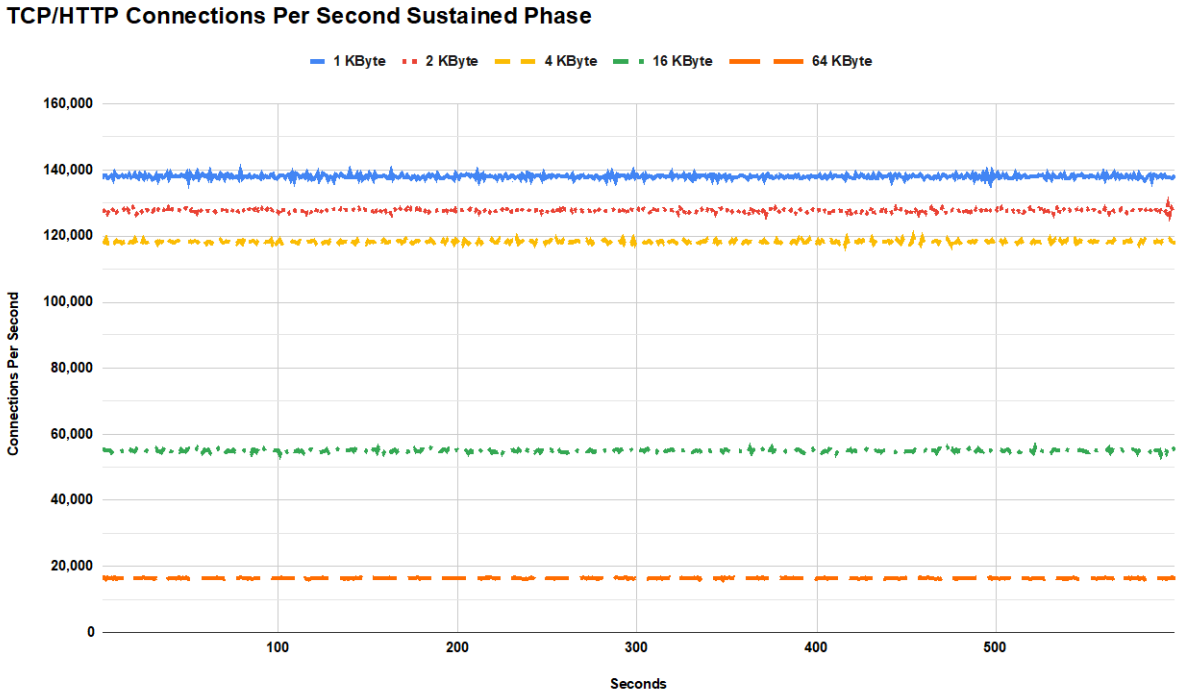
SECTION 7.8

TEST CASE	KPI	CPS 1K	CPS 16K	CPS 64K	TPUT 1K	TPUT 16K	TPUT 64K
HTTPS Transaction Latency	TTFB Average (msec)	1.43	1.85	1.93	0.99	1.88	2.68
	TTFB Minimum (msec)	0	0	0	0	0	0
	TTFB Maximum (msec)	30	32	38	29	30	31
	TTLB Average (msec)	1.58	2.11	3.58	0.98	2.03	4.57
	TTLB Minimum (msec)	0	0	0	0	0	0
	TTLB Maximum (msec)	30	33	46	29	31	36

SECTION 7.9

TEST CASE	KPI	1K
Concurrent TCP/HTTPS Connection Capacity	CC	79,800

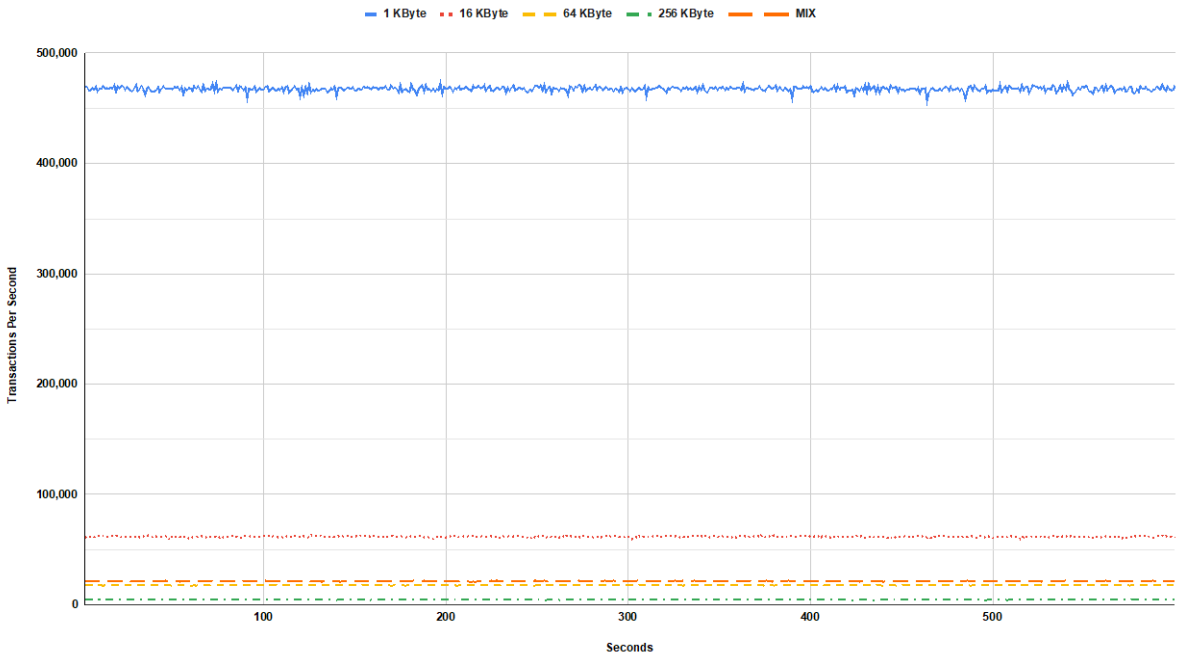
GRAPHS



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

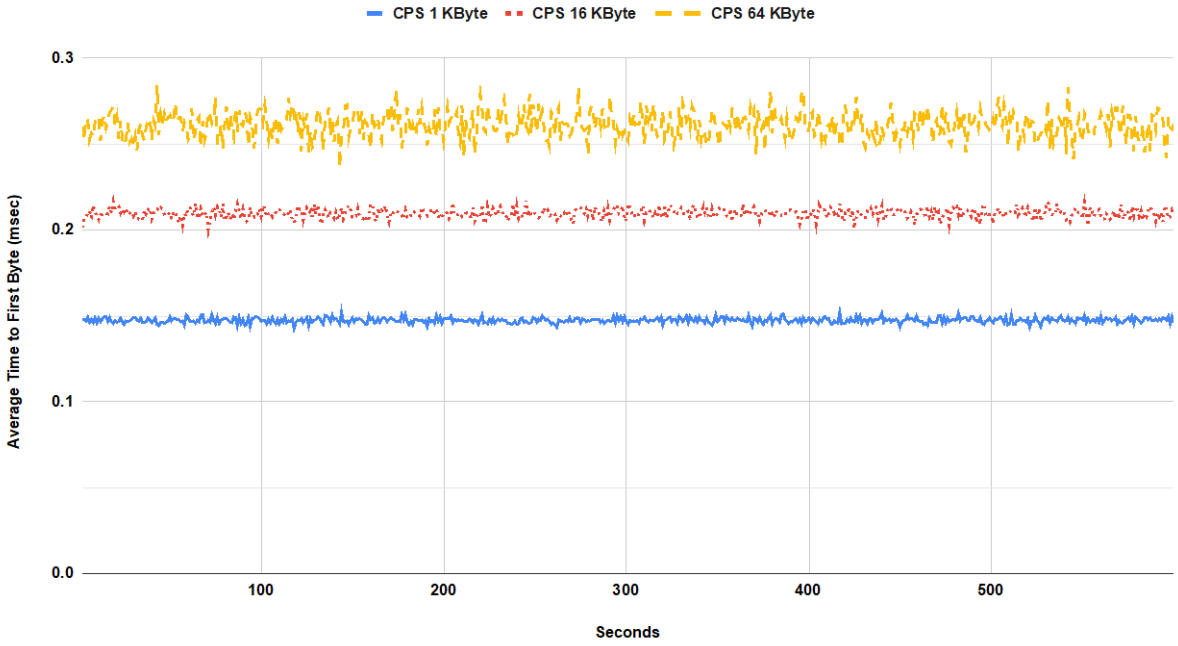
HTTP Throughput Sustained Phase

HTTP Transactions Per Second Sustained Phase

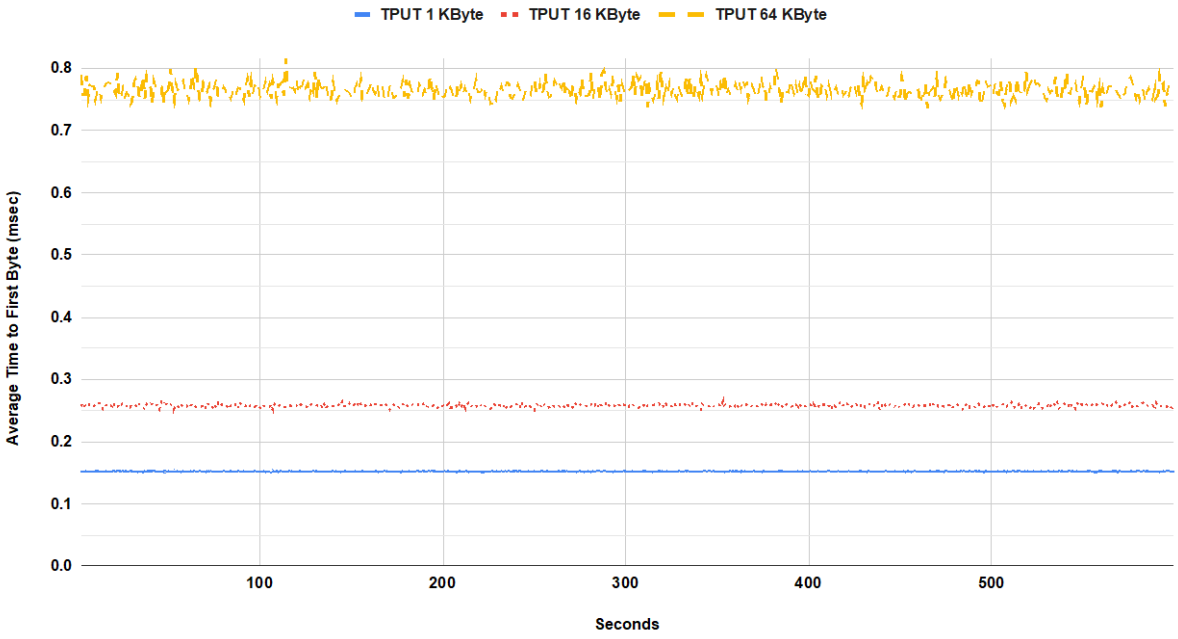


Sustainable throughput for of the DUT/SUT for HTTP transactions varying the HTTP response object size.

TCP/HTTP Transaction Latency Connections Per Second Sustained Phase

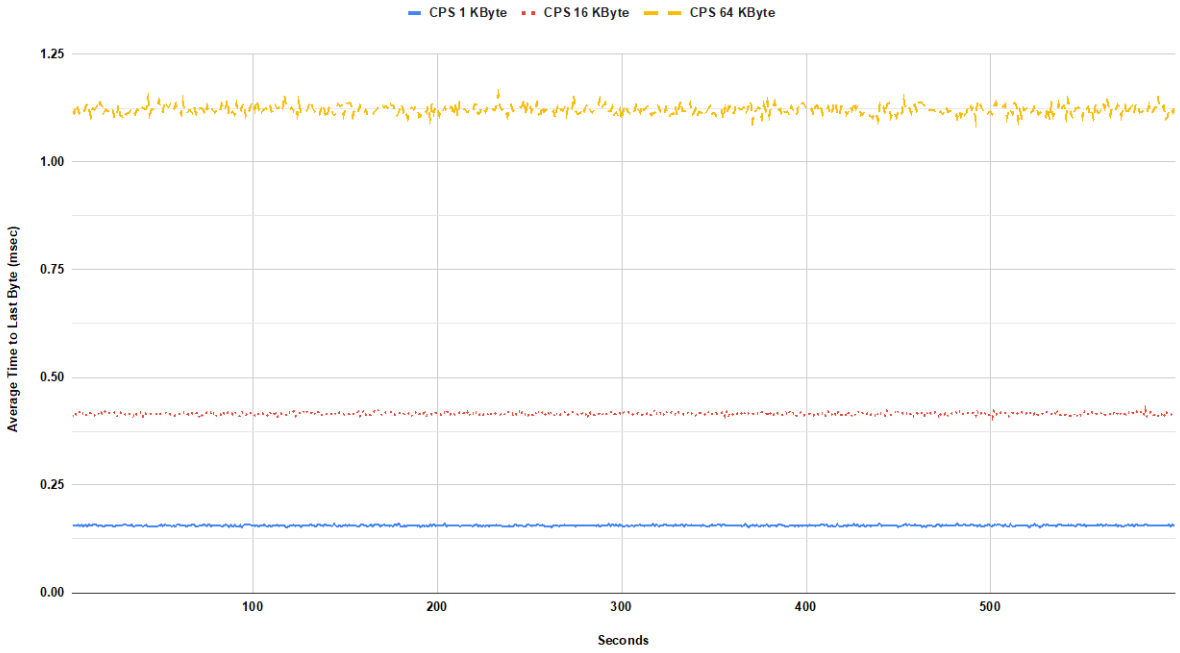


TCP/HTTP Transaction Latency Throughput Sustained Phase

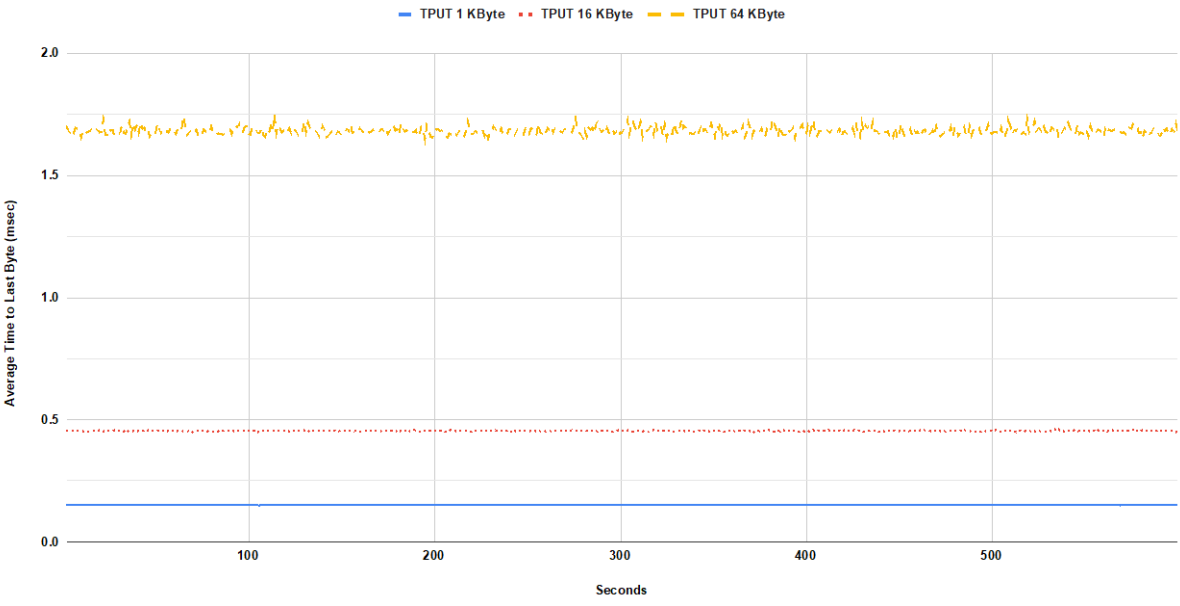


Average HTTP transaction latency time to first byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

TCP/HTTP Transaction Latency Connections Per Second Sustained Phase

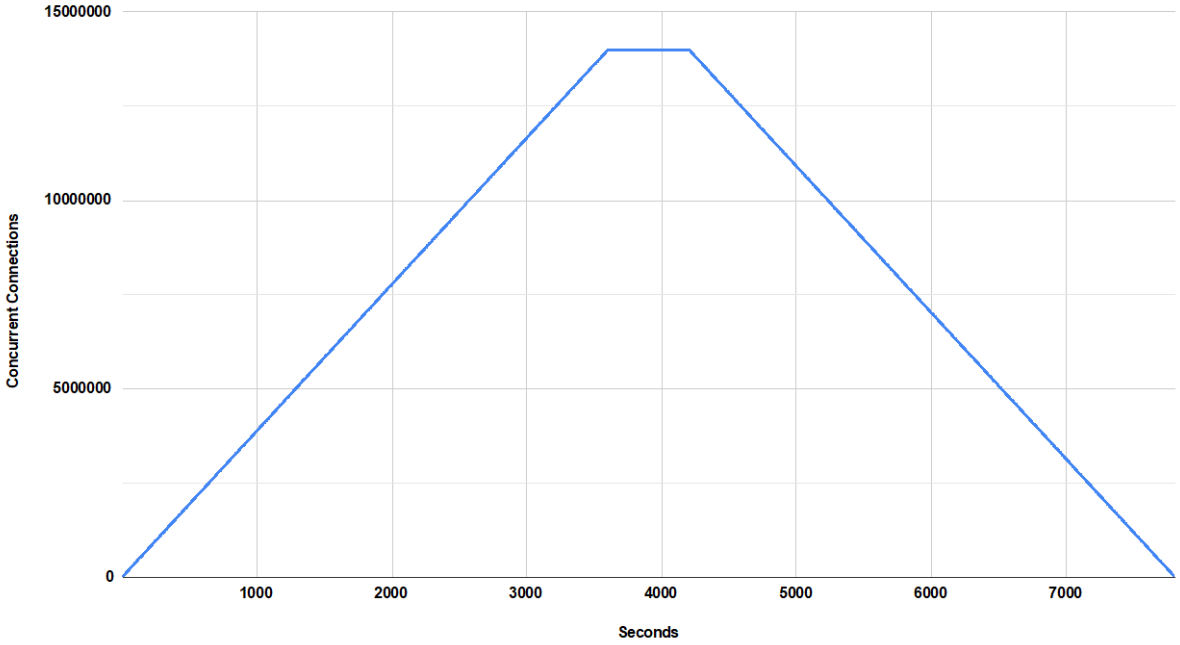


TCP/HTTP Transaction Latency Throughput Sustained Phase



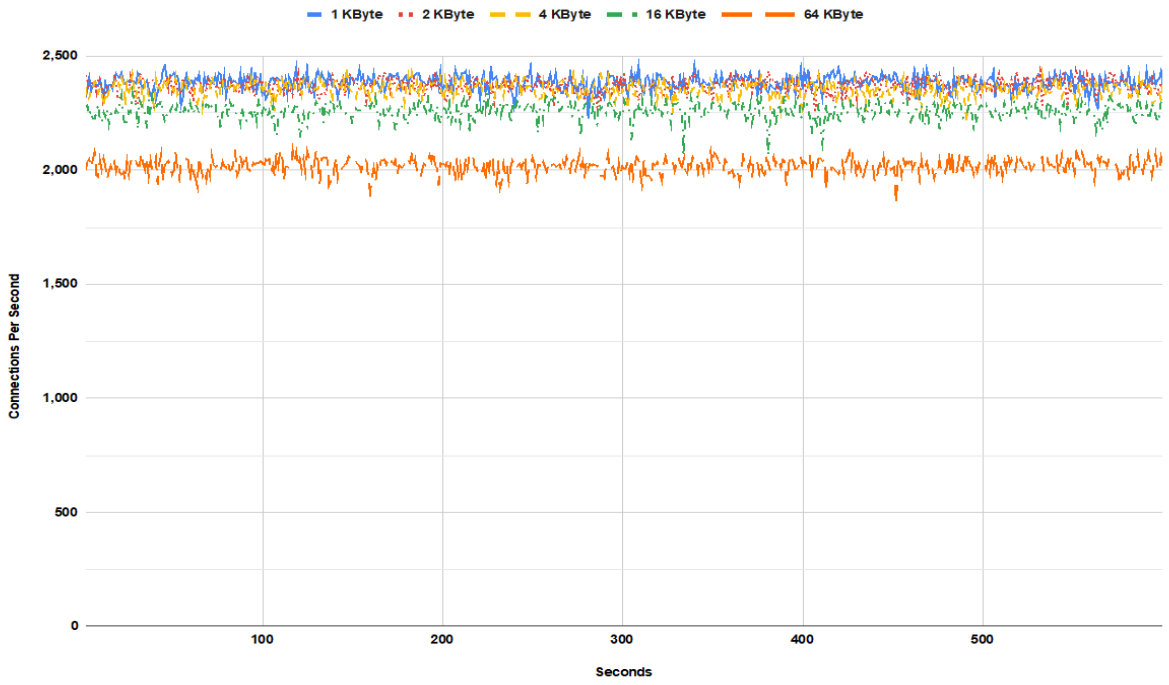
Average HTTP transaction latency time to last byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

Concurrent TCP/HTTP Connection Capacity

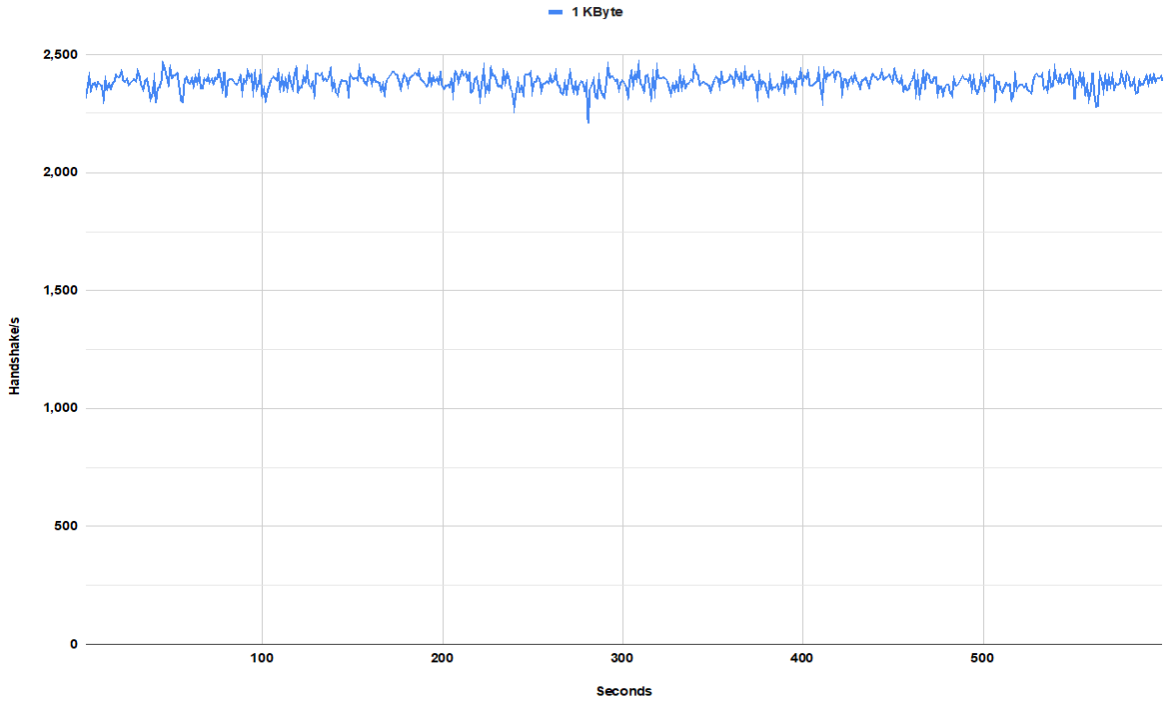


Number of concurrent TCP connections that the DUT/SUT sustains when using HTTP traffic.

TCP/HTTPS Connections Per Second Sustained Phase

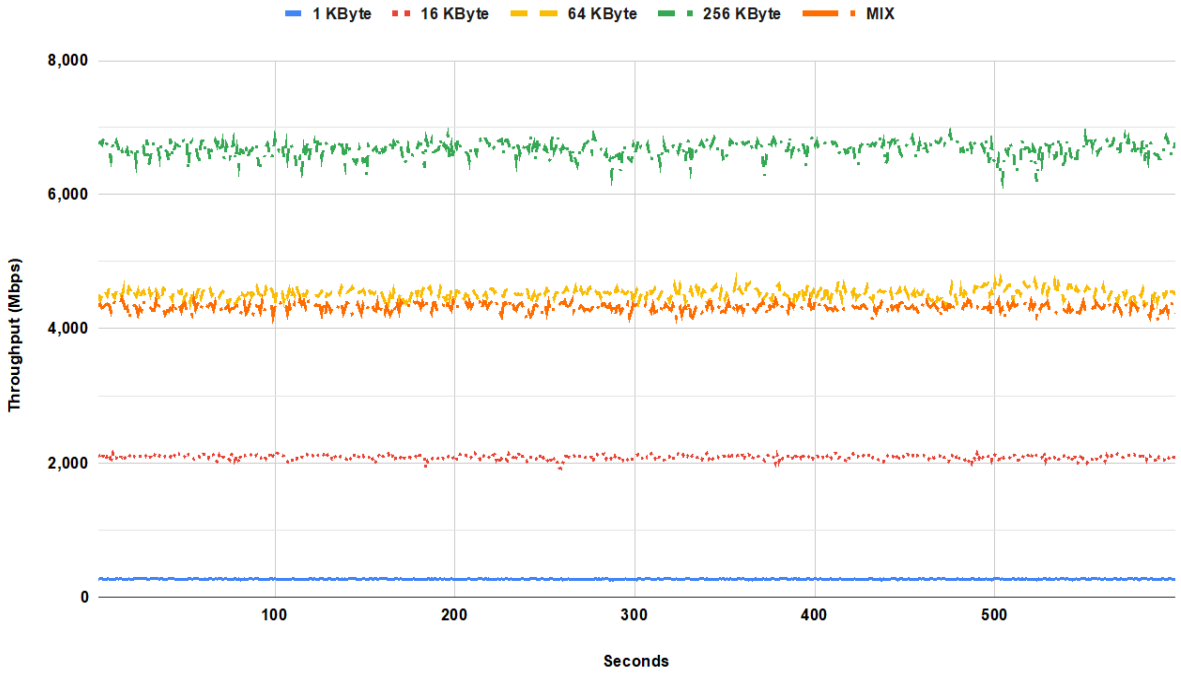


TCP/HTTPS TLS Handshake Rate Sustained Phase

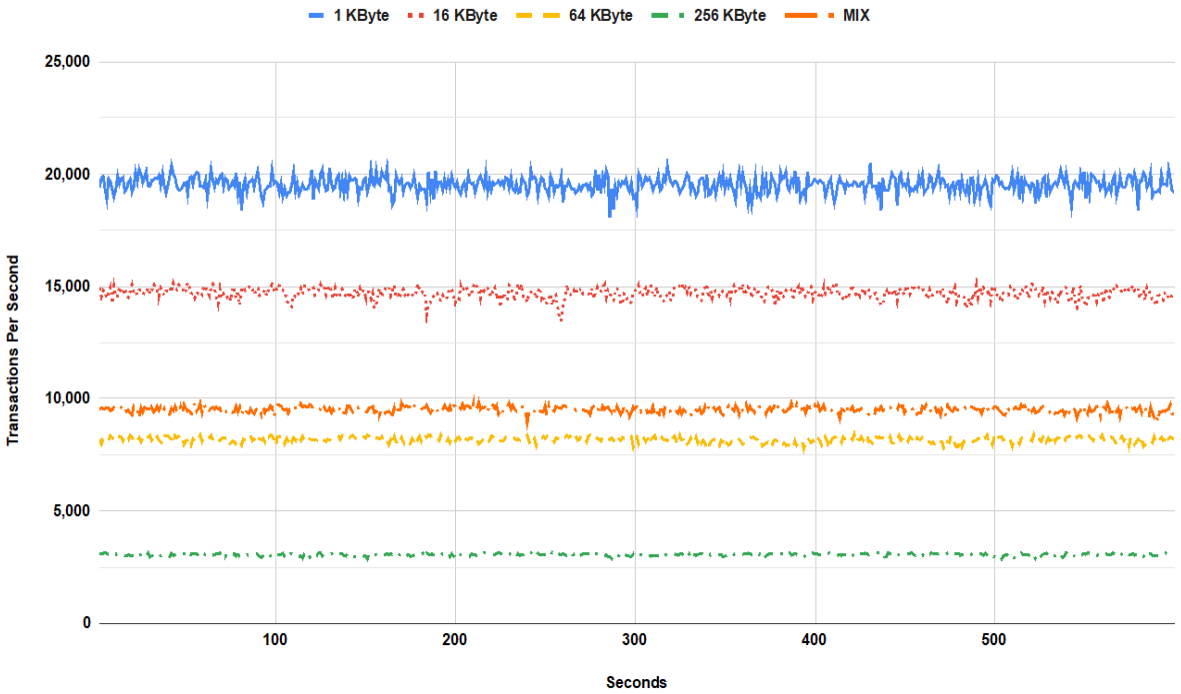


Sustainable SSL/TLS session establishment rate supported by the DUT/SUT under different throughput load conditions.

HTTPS Throughput Sustained Phase

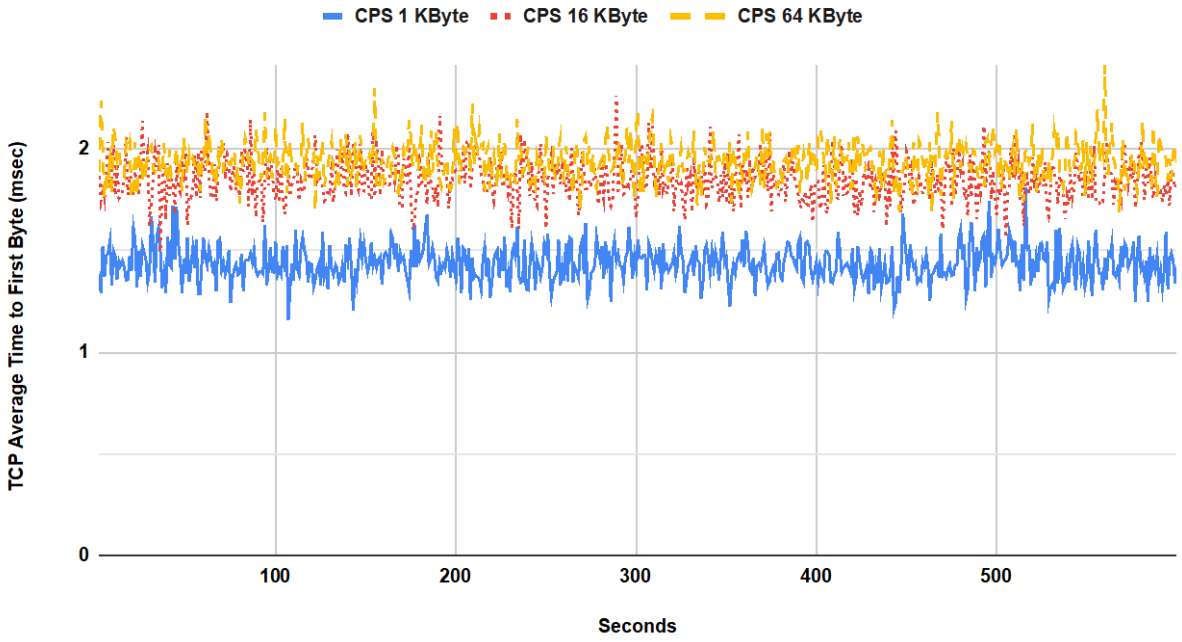


HTTPS Transactions Per Second Sustained Phase

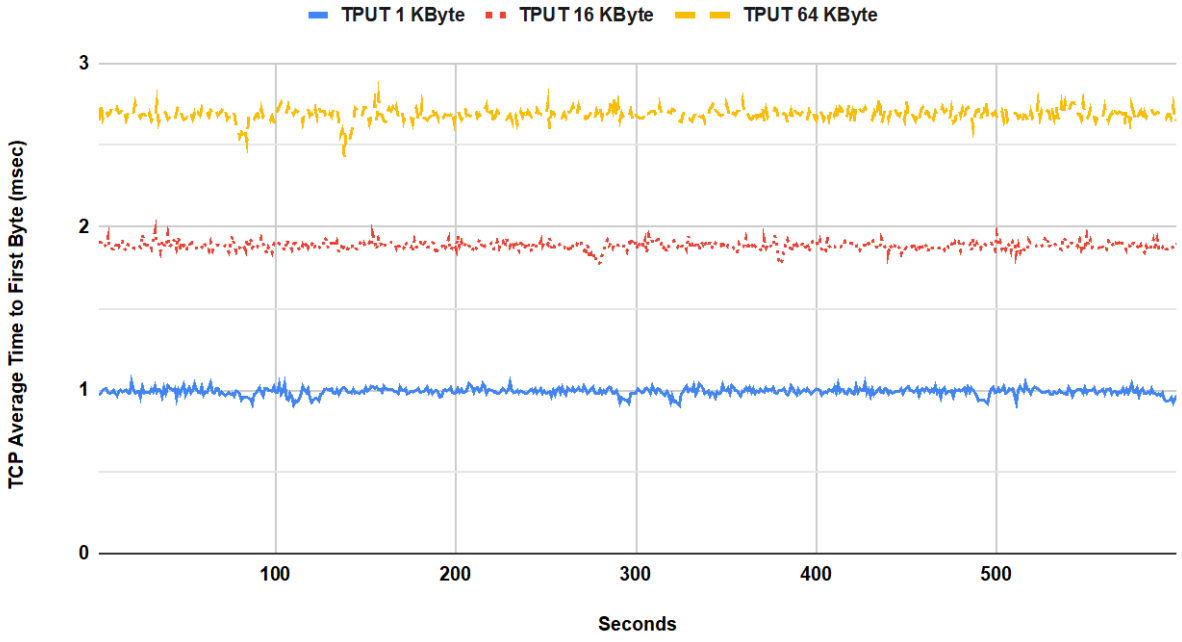


Sustainable throughput for of the DUT/SUT for HTTPS transactions varying the HTTPS response object size.

TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase

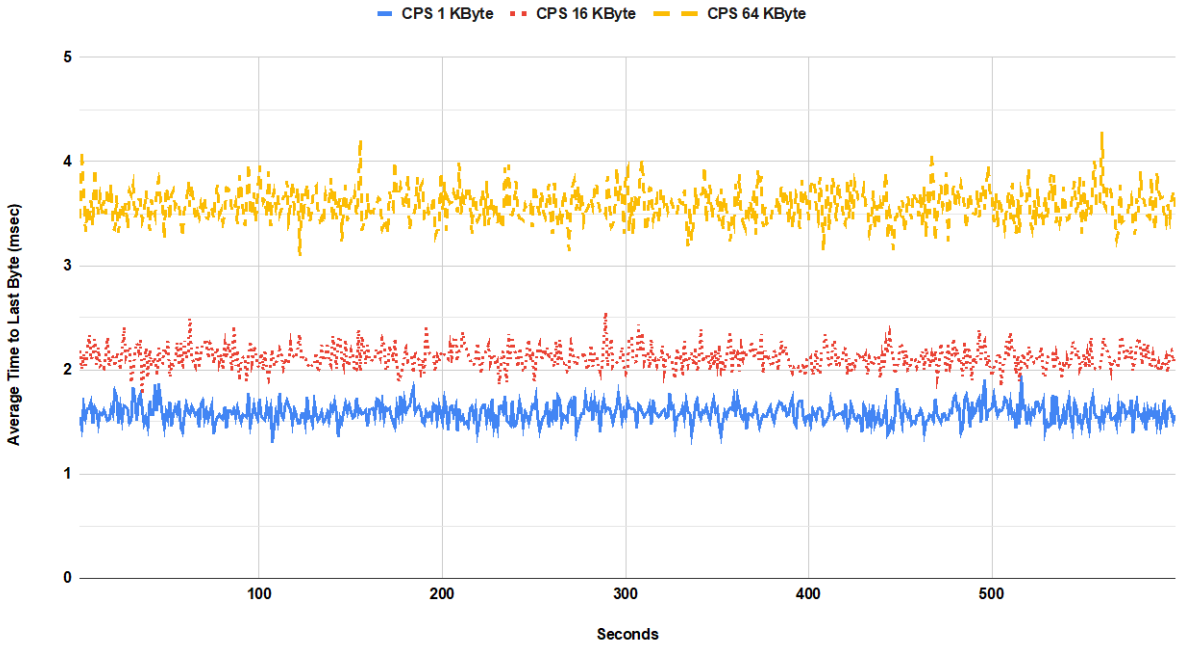


TCP/HTTPS Transaction Latency Throughput Sustained Phase

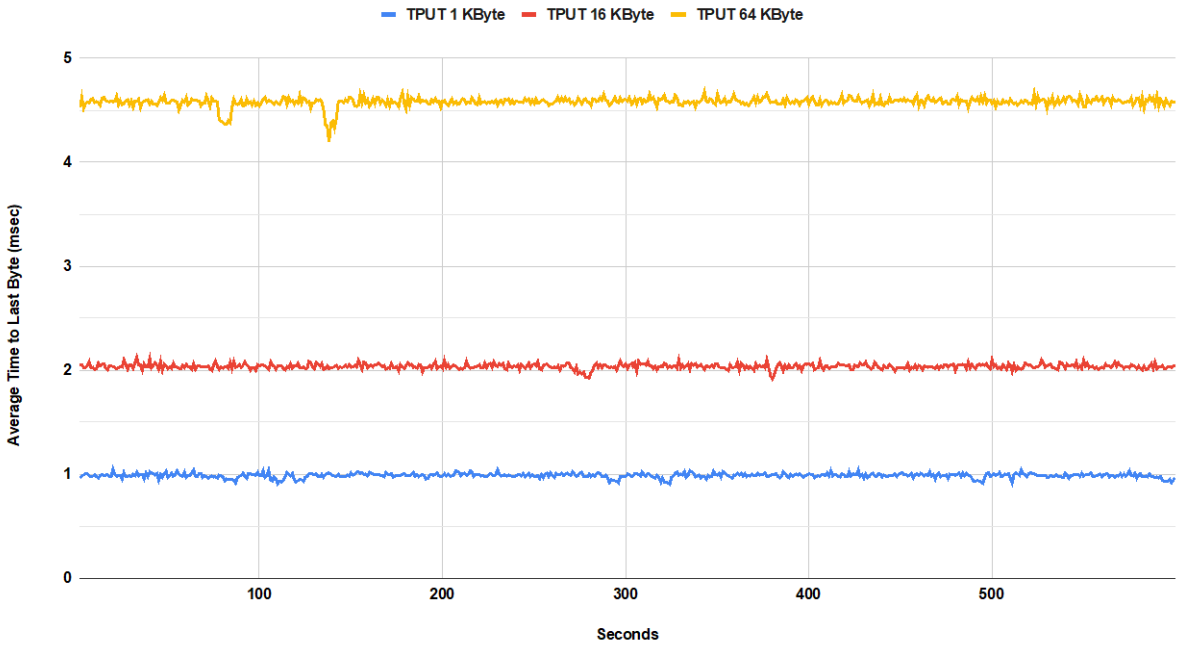


Average HTTPS transaction latency time to first byte under different HTTPS response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase

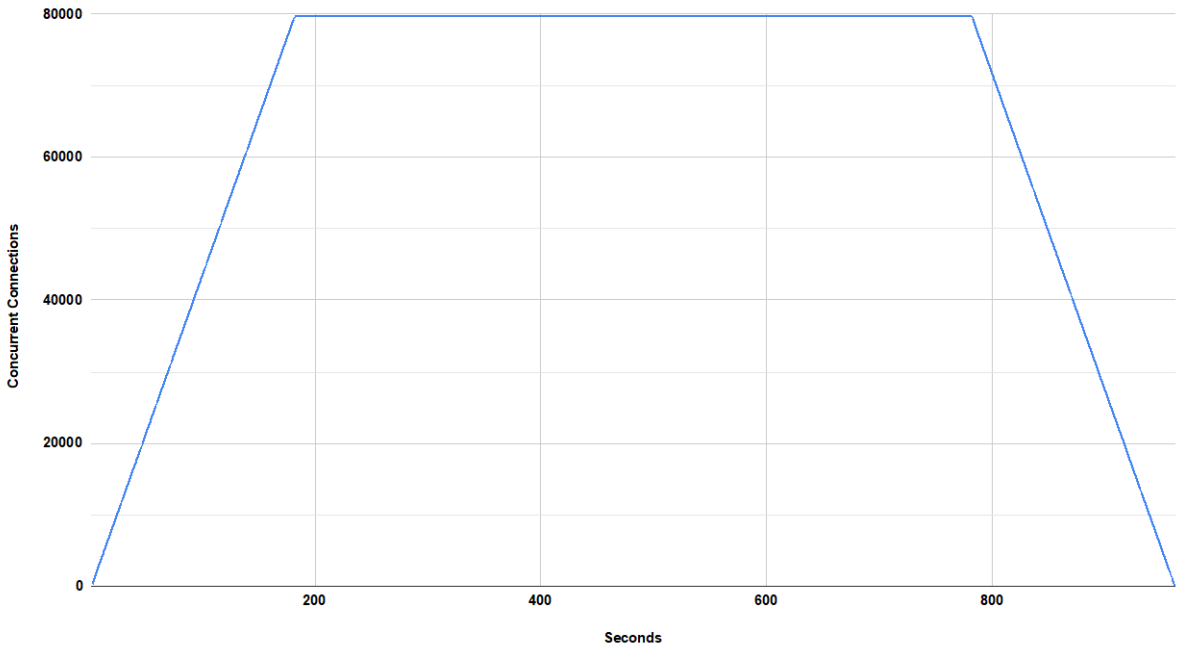


TCP/HTTPS Transaction Latency Throughput Sustained Phase



Average HTTPS transaction latency time to last byte 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



Number of concurrent TCP connections that the DUT/SUT sustains when using HTTPS traffic.

APPENDICES

APPENDIX 1: KPI KEY

The following table contains possible KPIs and their meanings.

KPI	MEANING	INTERPRETATION
CPS	TCP Connections Per Second	The average number of successfully established TCP connections per second between hosts across the DUT/SUT, or between hosts and the DUT/SUT. The TCP connection must be initiated via a TCP 3-way handshake (SYN, SYN/ACK, ACK). Then the TCP session data is sent. The TCP session MUST be closed via either a TCP 3 way close (FIN, FIN/ACK, ACK), or a TCP 4 way close (FIN, ACK, FIN, ACK), and not by a RST.
HR	TLS Handshake Rate	The average number of successfully established TLS connections per second between hosts across the DUT/SUT, or between hosts and the DUT/SUT.
TPUT	Inspected Throughput	The number of bits per second of allowed traffic a DUT/SUT can be observed to transmit to the correct destination interface(s) in response to a specified offered load (defined in [RFC2647]). The throughput benchmarking tests SHOULD measure the average OSI model Layer 2 throughput value.
TPS	Application Transactions Per Second	The average number of successfully completed transactions per second. For a particular transaction to be considered successful, all data must have been transferred in its entirety. In case of HTTP(S) transaction, it must have a valid status code, and the appropriate FIN, FIN/ACK sequence must have been completed.
TTFB	Time to First Byte	TTFB is the elapsed time between the start of sending the TCP SYN packet from the client and the client receiving the first packet of application data from the server or DUT/SUT. The benchmarking tests HTTP Transaction Latency and HTTPS Transaction Latency measure the minimum, average and maximum TTFB. The value SHOULD be expressed in millisecond.
TTLB	Time to Last Byte	URL Response time / TTLB is the elapsed time between the start of sending the TCP SYN packet from the client and the client receiving the last packet of application data from the server or DUT/SUT. The benchmarking tests HTTP Transaction Latency and HTTP Transaction Latency measure the minimum, average and maximum TTLB. The value SHOULD be expressed in millisecond.
CC	Concurrent TCP Connections	The aggregate number of simultaneous connections between hosts across the DUT/SUT, or between hosts and the DUT/SUT (defined in [RFC2647]).

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	435	0
Private CVE	33	33	0