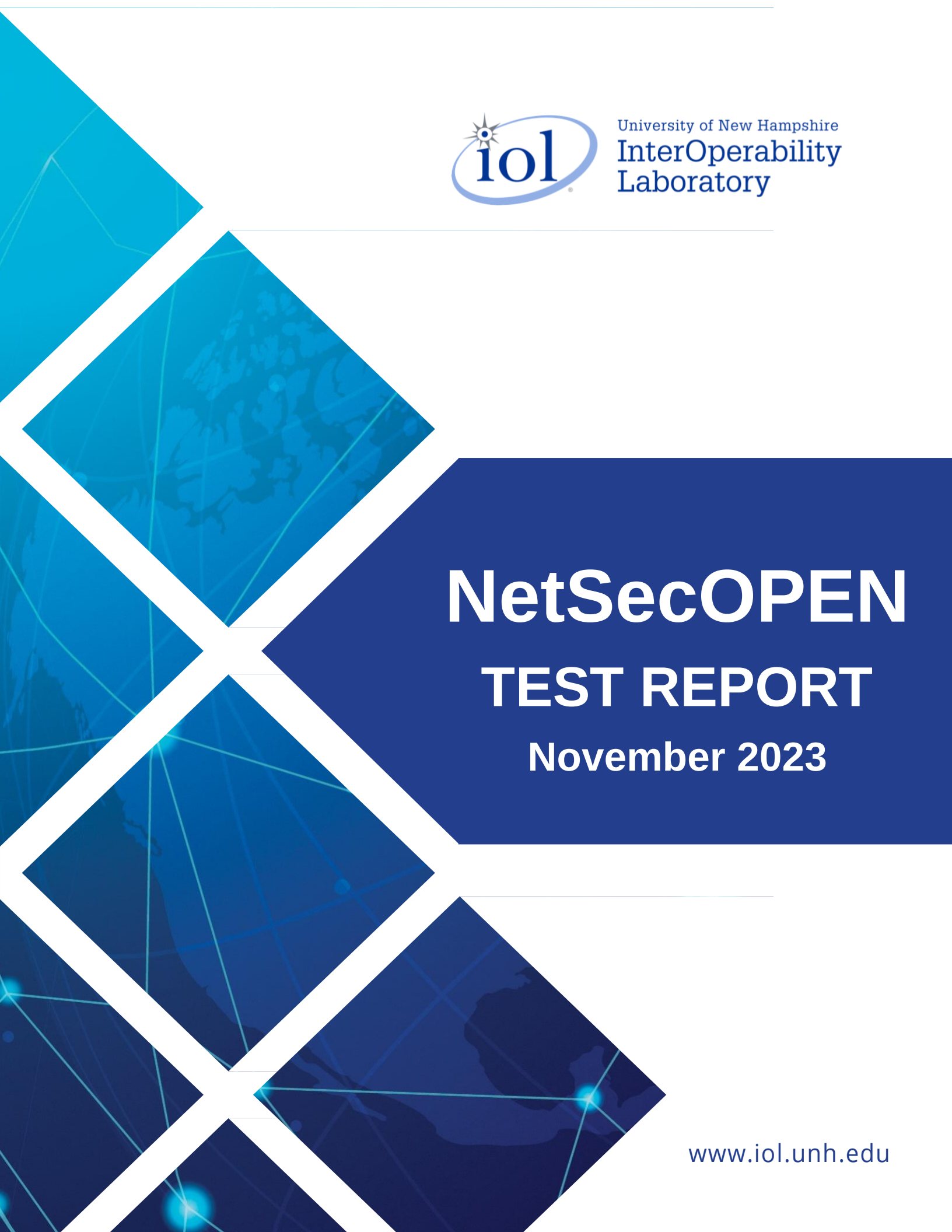


NetSecOPEN

TEST REPORT

November 2023

www.iol.unh.edu

SAMARESH NAIR
PALO ALTO NETWORKS
SNAIR@PALOALTONETWORKS.COM

DEVICE AND TEST PLAN INFORMATION	
Device Under Test (DUT)	PA-450
Test Specification/Suite	Benchmarking Methodology for Network Security Device Performance RFC 9411
UNH-IOL Test Result ID	37520

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

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

Digitally signed by Chris Brown
Date: 2024.02.13 16:15:09 -05'00'

TESTING NOTES

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

NOTES
Palo Alto's WildFire is a cloud-based malware protection engine. It was required to have scheduled update occurrences for this feature set to "real-time". Therefore, this dynamic update was upgraded throughout the testing process. At the time of writing this report, WildFire version 816918-820718 is installed on the device under test. The test tool was configured with delayed TCP ACKs of 200 milliseconds for the education and healthcare traffic mixes. It was observed that the tool would occasionally send ACKs later than expected. This caused retransmissions to be sent from the DUT and duplicate ACKs sent from the test tool resulting in the amount of received data to be larger than data transmitted.

REVISION HISTORY

The following table contains a revision history for this report.

REVISION	DATE	AUTHOR	EXPLANATION
1.0	11/01/2023	Chris Brown	Initial version
2.0	11/03/2023	Chris Brown	Updated Security Effectiveness Summary to better reflect block rate percentages
3.0	12/21/2023	Chris Brown	Updated report to include malware and CVE omitted samples
4.0	02/13/2024	Chris Brown	Updated report to indicate number of ACLs, logging, and notes regarding traffic mixes delayed ACKs

DEVICE INFORMATION

COMPONENT	DESCRIPTION
Device Name	PA-450
UNH-IOL Device Identification Number	FW-PALO-0000029808
Device Model	PA-450
Device Firmware	11.0.2-h2
Antivirus	4592-5109
Applications and Threats	8759-8313
WildFire	Information can be found at Testing Notes
Interfaces Tested	Ethernet1/1, ethernet1/2, ethernet1/5, ethernet1/6
Interfaces Speed	1G

DEVICE ENABLED FEATURES

FEATURE	STATUS	
	ENABLED	DISABLED
TLS Inspection	✓	
IDS/IPS	✓	
Anti-Spyware	✓	
Anti-Virus	✓	
Anti-Botnet	✓	
Anti-Evasion	✓	
Web Filtering		✓
Data Loss Protection (DLP)		✓
DDoS Protection		✓
Certificate Validation		✓
Application Identification	✓	
Logging and Reporting	✓	

DEVICE ACL RULES

RULE TYPE	ACTION	# OF RULES
Application Layer	Block	10
Transport Layer	Block	50
IP Layer	Block	50
Application Layer	Allow	10
Transport Layer	Allow	1
IP Layer	Allow	1

TEST TOOL AND ENVIRONMENT INFORMATION

COMPONENT	DESCRIPTION	
Test Equipment Vendor	Ixia	
Hardware Name	PerfectStorm One	
Hardware Firmware	9.20.2700.23	
Hardware Interface Type	1G	
Application Software Name	BreakingPoint	
Application Software Version	9.20.115.12	
Application and Threat Intelligence (ATI) Strikepack Version	2023-17	
Client IP Subnet 1	10.10.0.0/21	
Server IP Subnet 1	10.11.0.0/21	
Client IP Subnet 2	10.12.0.0/21	
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 Test Equipment Vendor

SECURITY EFFECTIVENESS SUMMARY

SCENARIO	TOTAL	BLOCKED	ALLOWED	BLOCK RATE
Public CVE	1,381	1,360	21	98.48%
Private CVE	180	178	2	98.89%
Malware	3,809	3,809	0	100%
Evasions	19	19	0	100%
More information can be found at APPENDIX 2				

SECURITY TESTING UNDER LOAD		
Traffic Mix Type:	Healthcare	Education
TPUT (Mbps)	202	220
TPS	809	1,077
Block Rate	100%	100%
More Information can be found at APPENDIX 3		

KPI RESULT SUMMARY

SECTION 7.1

TEST CASE	KPI	HEALTHCARE MIX	EDUCATION MIX
Application Traffic Mix	TPUT (Mbps)	217	239
	TPS	865	1,185

SECTION 7.2

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTP Connections Per Second	CPS	5,992	5,701	5,548	3,900	1,300

SECTION 7.3

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTP Inspected Throughput	TPUT (Mbps)	98	679	1,049	1,553	858
	TPS	8,333	4,860	1,900	636	1,900

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)	1.36	1.35	1.30	1.29	1.30	1.46
	TTFB Minimum (msec)	1.30	1.30	1.23	1.26	1.26	1.36
	TTFB Maximum (msec)	1.44	1.42	1.38	1.33	1.35	1.58
	TTLB Average (msec)	1.37	1.79	2.57	1.29	1.67	3.22
	TTLB Minimum (msec)	1.31	1.73	2.47	1.26	1.64	2.97
	TTLB Maximum (msec)	1.45	1.87	5.64	1.33	1.73	7.18

SECTION 7.5

TEST CASE	KPI	1K
Concurrent TCP/HTTP Connection Capacity	CC	298,900

SECTION 7.6

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTPS Connections Per Second	CPS	1,690	1,646	1,600	1,290	780
	HR	1K				
		1,690				

SECTION 7.7

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTPS Inspected Throughput	TPUT (Mbps)	70	413	662	800	640
	TPS	4,966	2,900	1,200	361	1,407

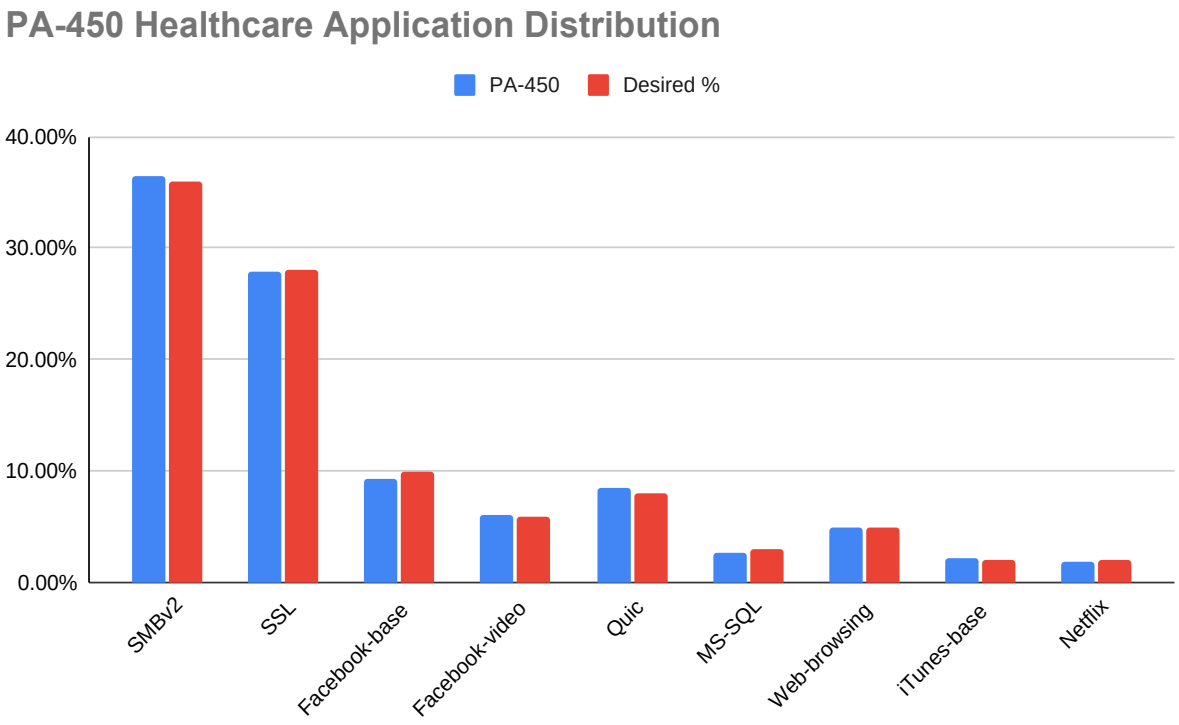
SECTION 7.8

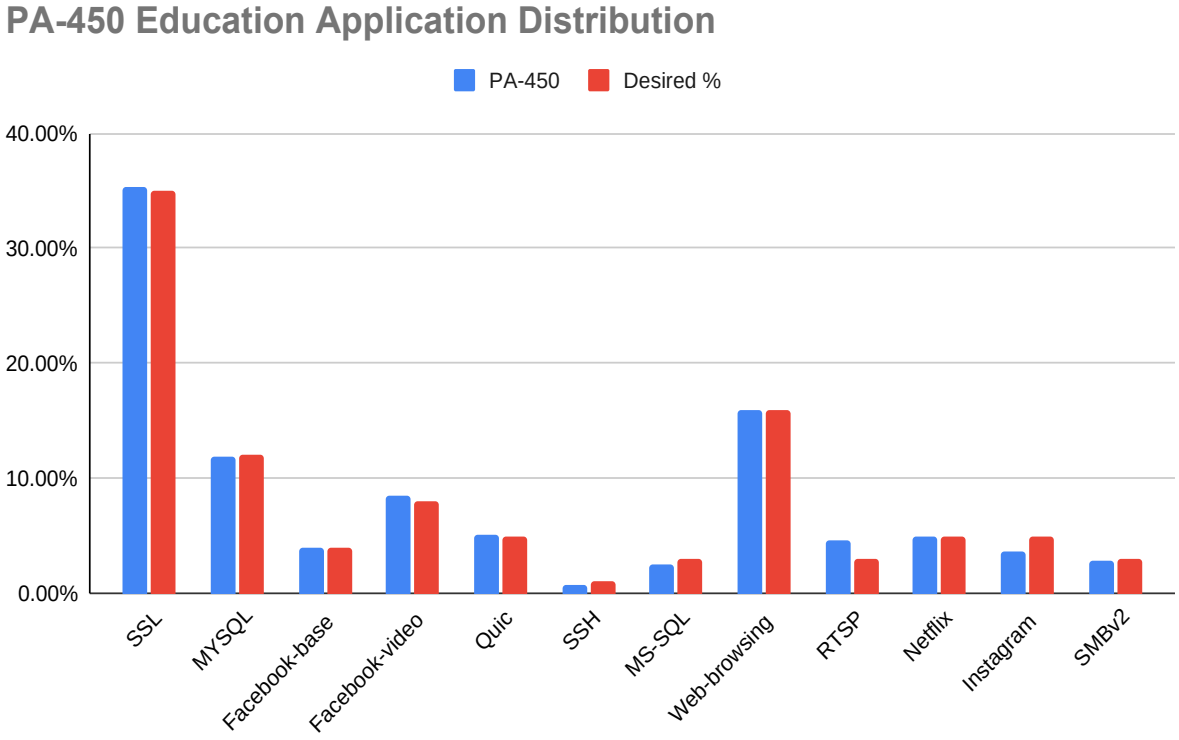
TEST CASE	KPI	CPS 1K	CPS 16K	CPS 64K	TPUT 1K	TPUT 16K	TPUT 64K
TCP/HTTPS Transaction Latency	TTFB Average (msec)	2.04	2.63	3.43	1.84	2.48	3.51
	TTFB Minimum (msec)	1.93	2.48	3.19	1.75	2.32	3.27
	TTFB Maximum (msec)	2.16	3.41	4.76	2.14	2.95	4.47
	TTLB Average (msec)	2.21	93.06	184.40	1.84	11.73	23.40
	TTLB Minimum (msec)	2.10	92.76	183.88	1.75	11.54	22.21
	TTLB Maximum (msec)	2.42	93.79	185.65	2.14	12.21	27.73

SECTION 7.9

TEST CASE	KPI	1K
Concurrent TCP/HTTPS Connection Capacity	CC	30,000

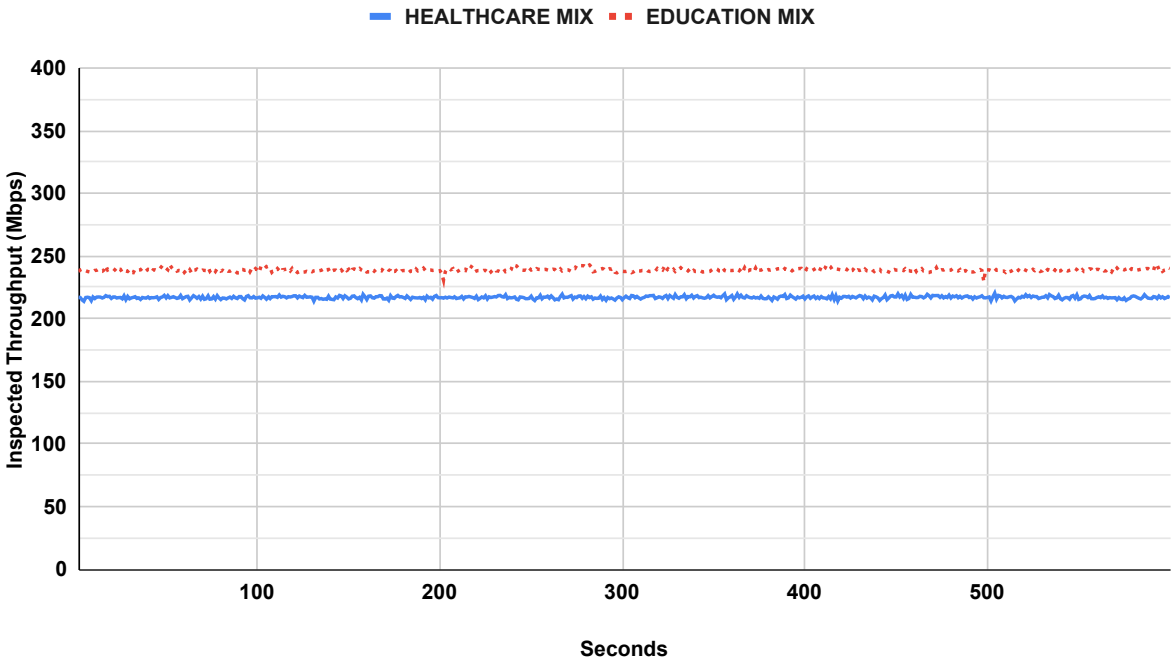
GRAPHS



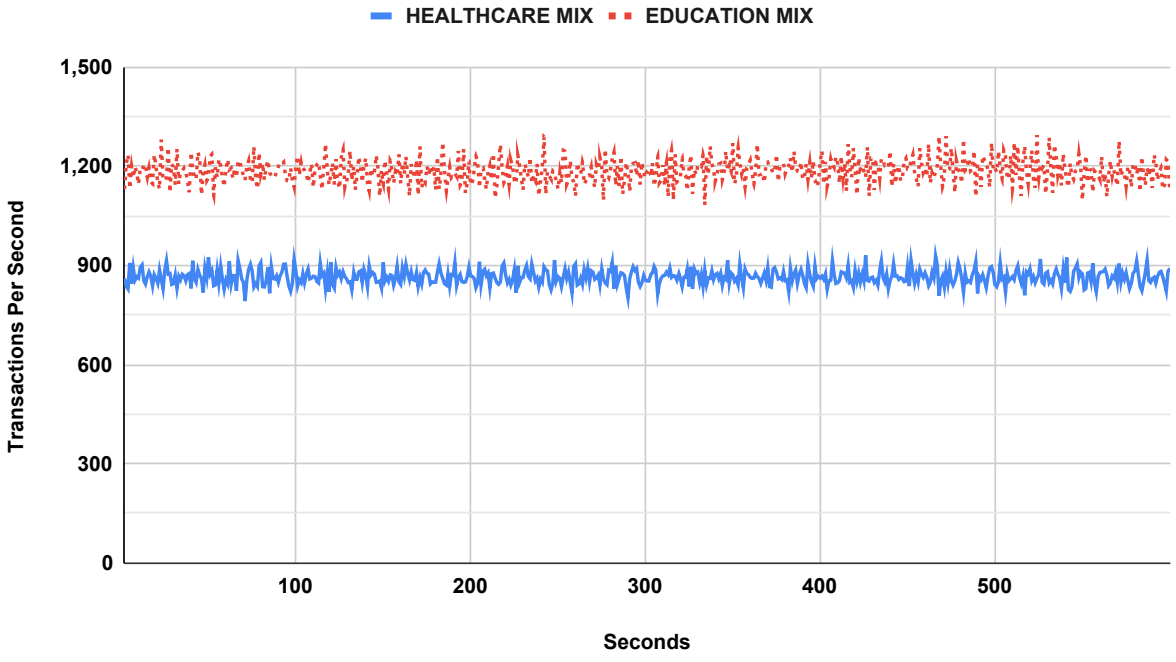


Comparison of desired Inspected Throughput and observed Inspected Throughput for each application within the traffic mixes.

Inspected Throughput Sustained Phase

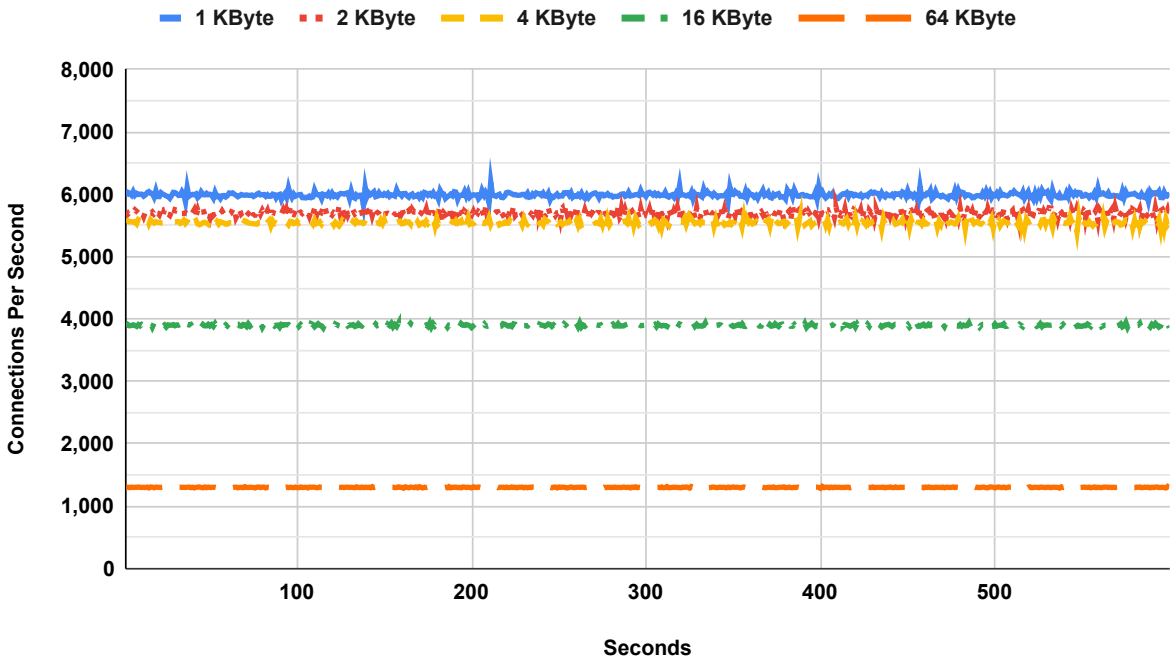


Transactions Per Second Sustained Phase



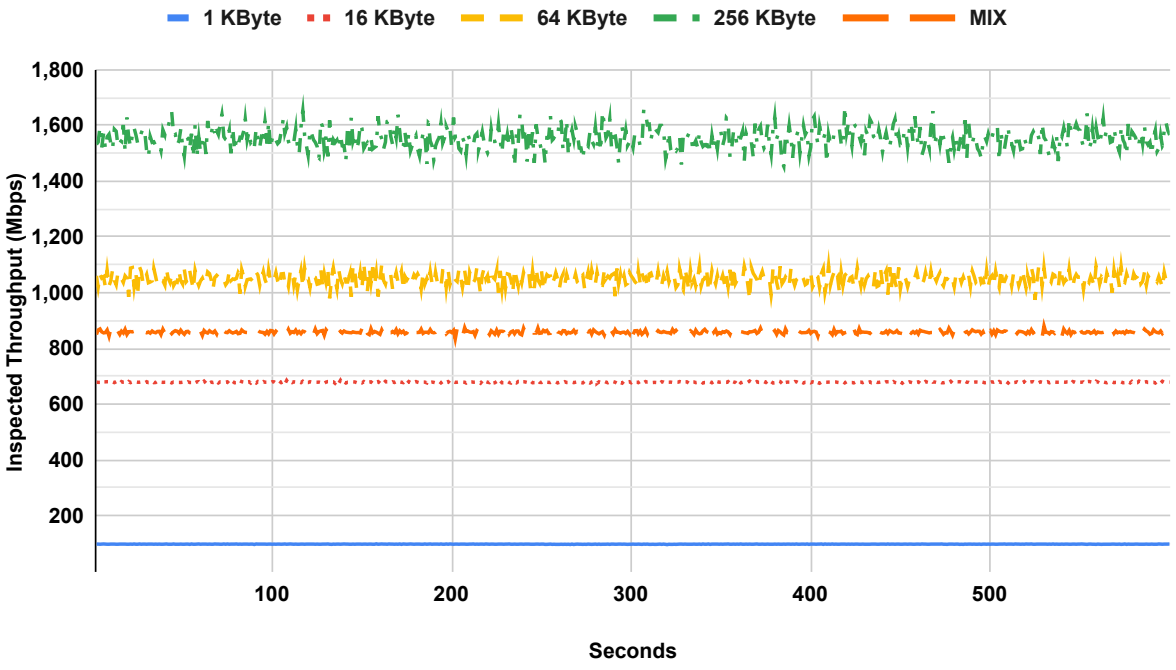
Sustainable inspected throughput of the DUT/SUT for Application Traffic Mixes.

TCP/HTTP Connections Per Second Sustained Phase

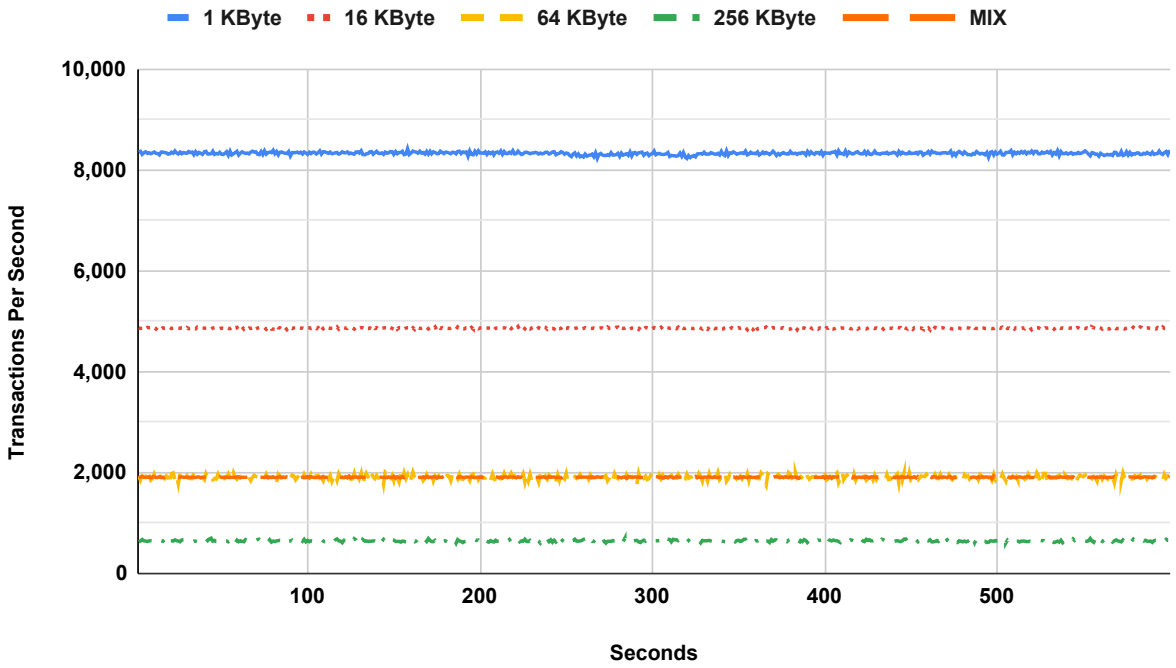


Sustainable TCP/HTTP connection establishment rate supported by the DUT/SUT under different throughput load conditions.

HTTP Inspected Throughput Sustained Phase

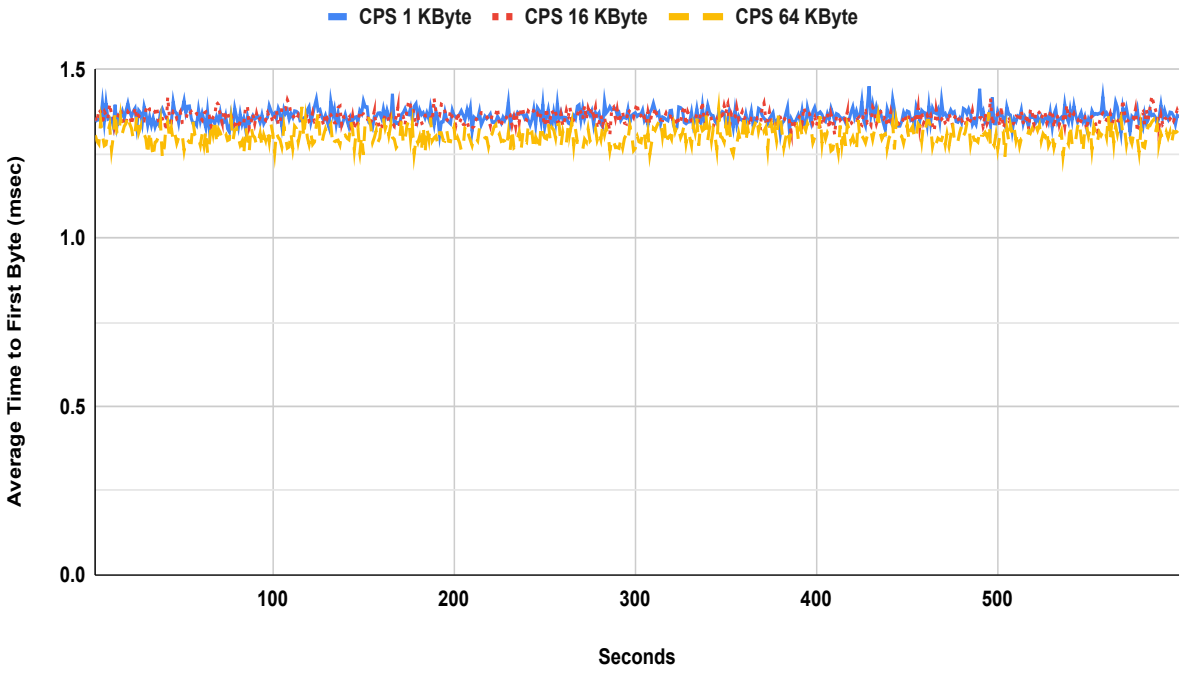


HTTP Transactions Per Second Sustained Phase

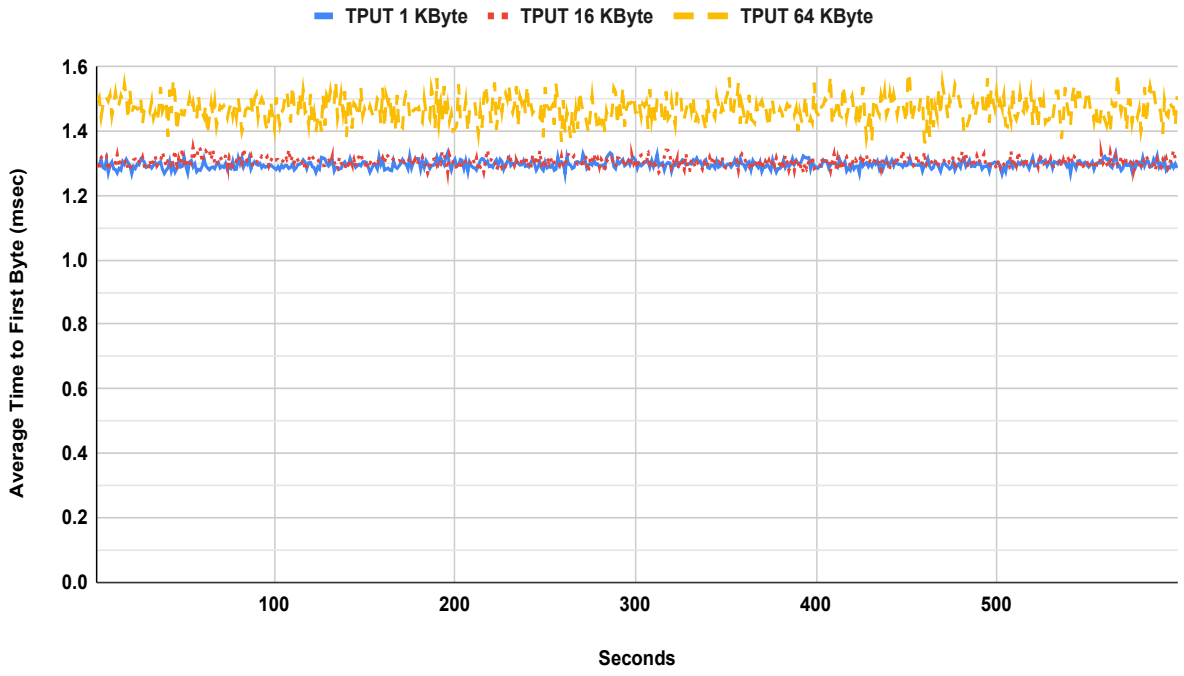


Sustainable inspected throughput of the DUT/SUT for HTTP transactions varying the HTTP response object size.

TCP/HTTP Transaction Latency Connections Per Second Sustained Phase

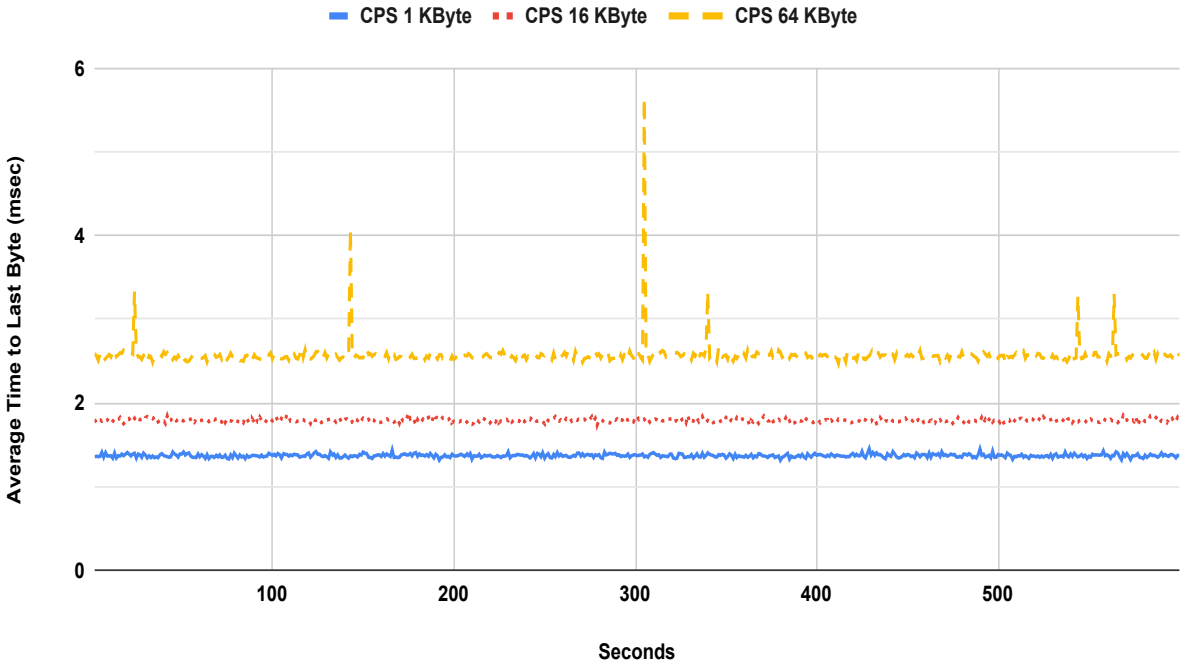


TCP/HTTP Transaction Latency Inspected Throughput Sustained Phase

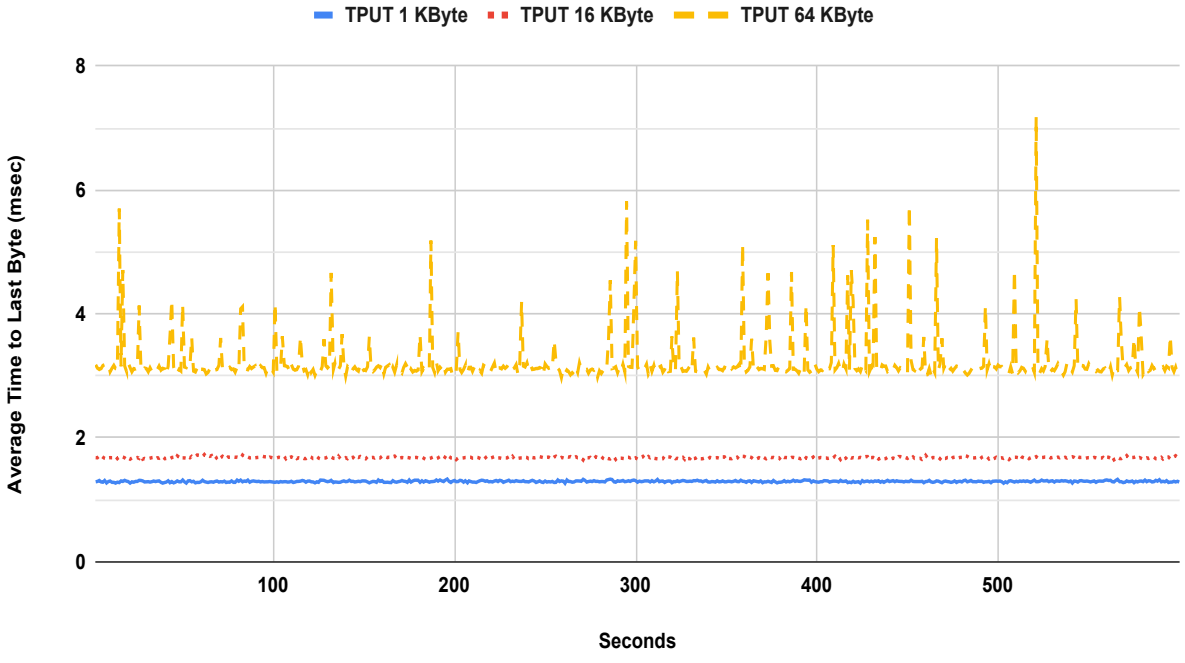


Average HTTP transaction latency time to first byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

TCP/HTTP Transaction Latency Connections Per Second Sustained Phase

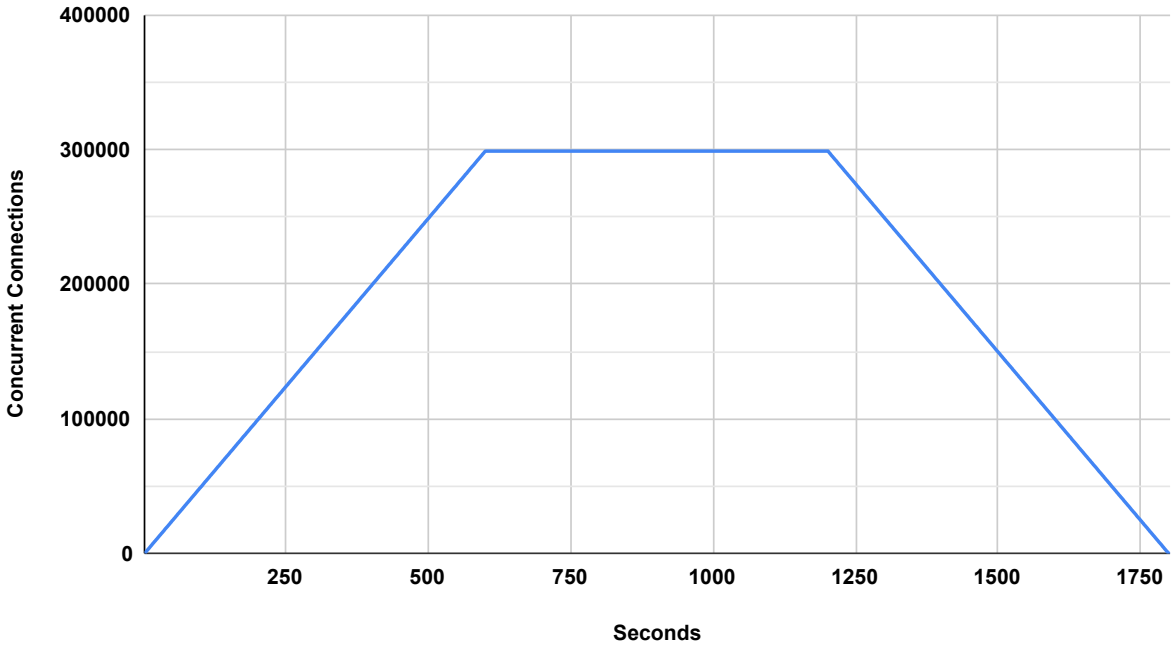


TCP/HTTP Transaction Latency Inspected Throughput Sustained Phase



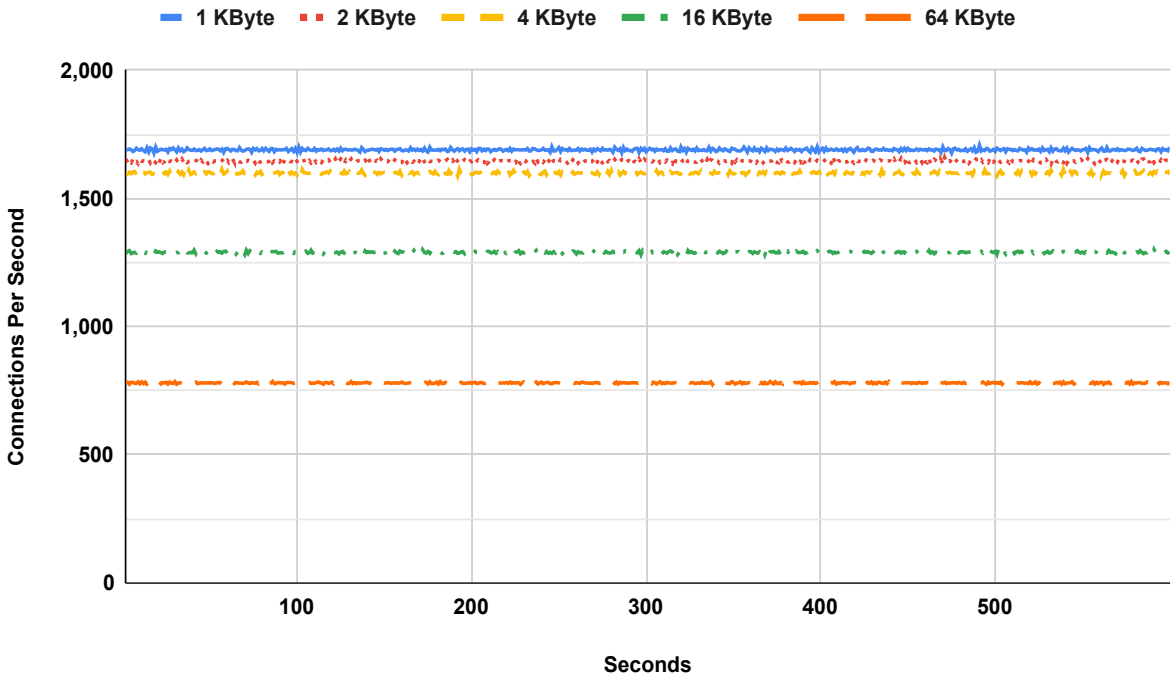
Average HTTP transaction latency time to last byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

Concurrent TCP/HTTP Connection Capacity

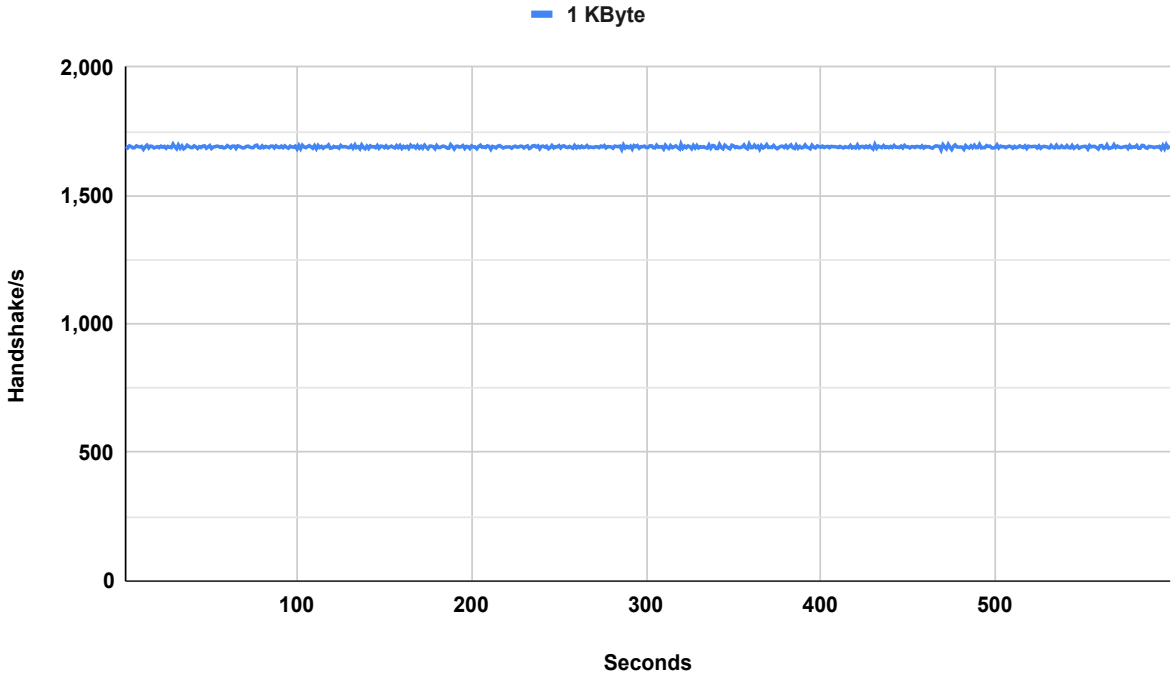


Number of concurrent TCP connections that the DUT/SUT sustains when using HTTP traffic.

TCP/HTTPS Connections Per Second Sustained Phase

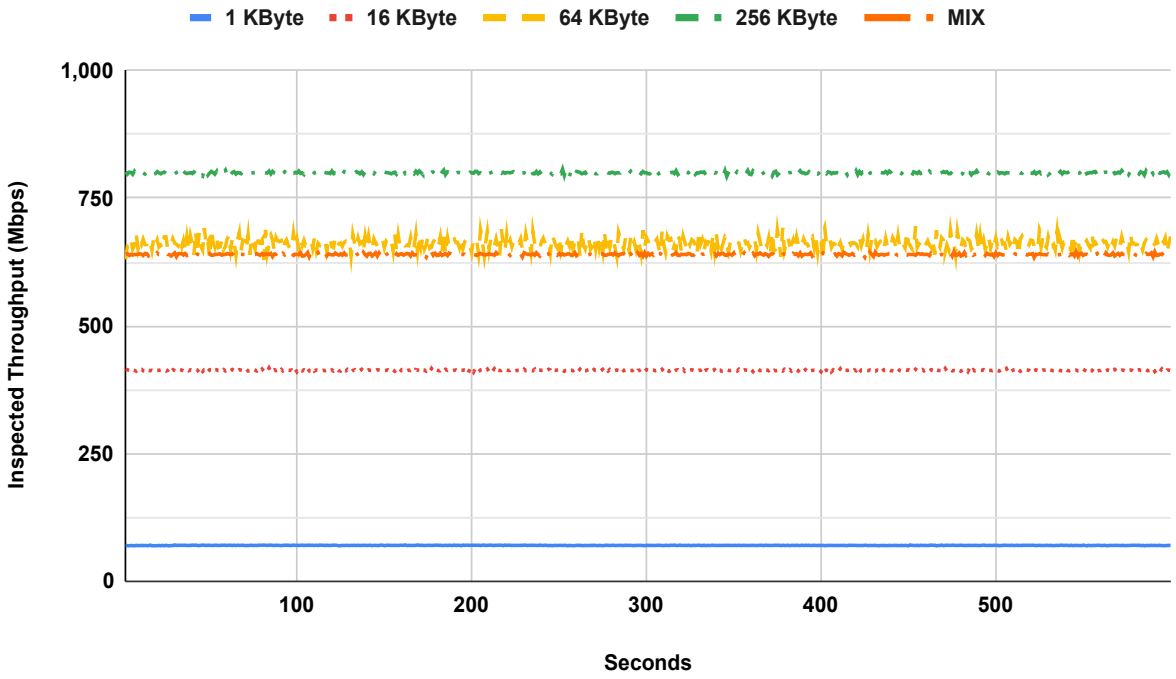


TCP/HTTPS TLS Handshake Rate Sustained Phase

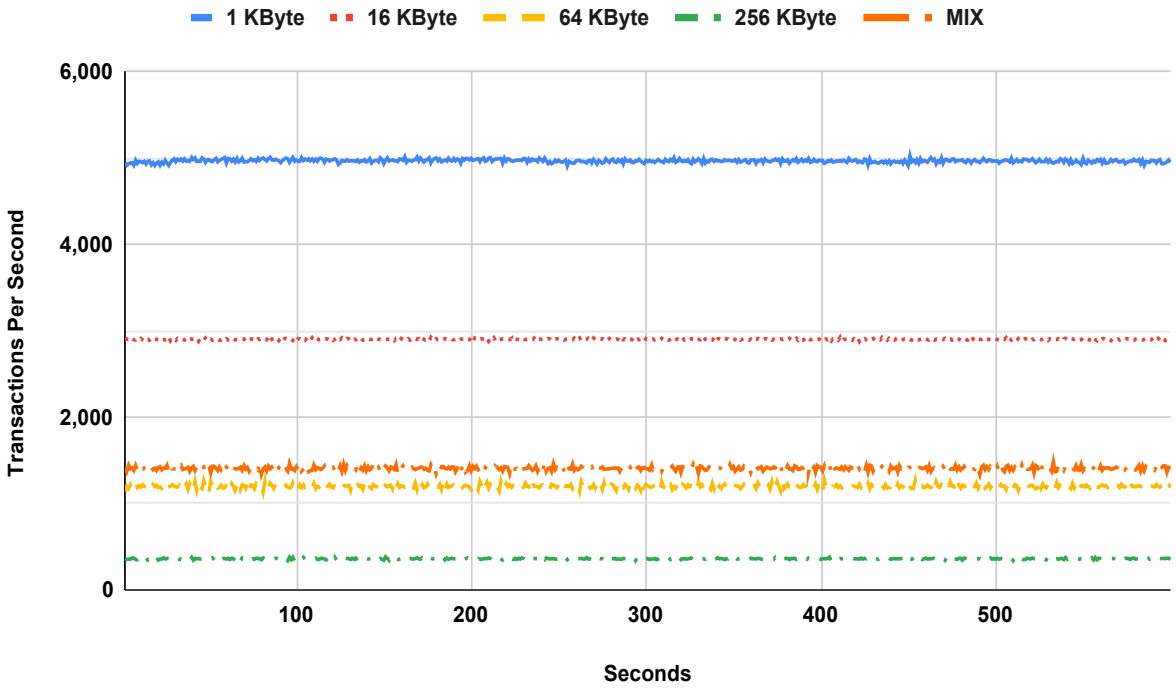


Sustainable SSL/TLS session establishment rate supported by the DUT/SUT under different throughput load conditions.

HTTPS Inspected Throughput Sustained Phase

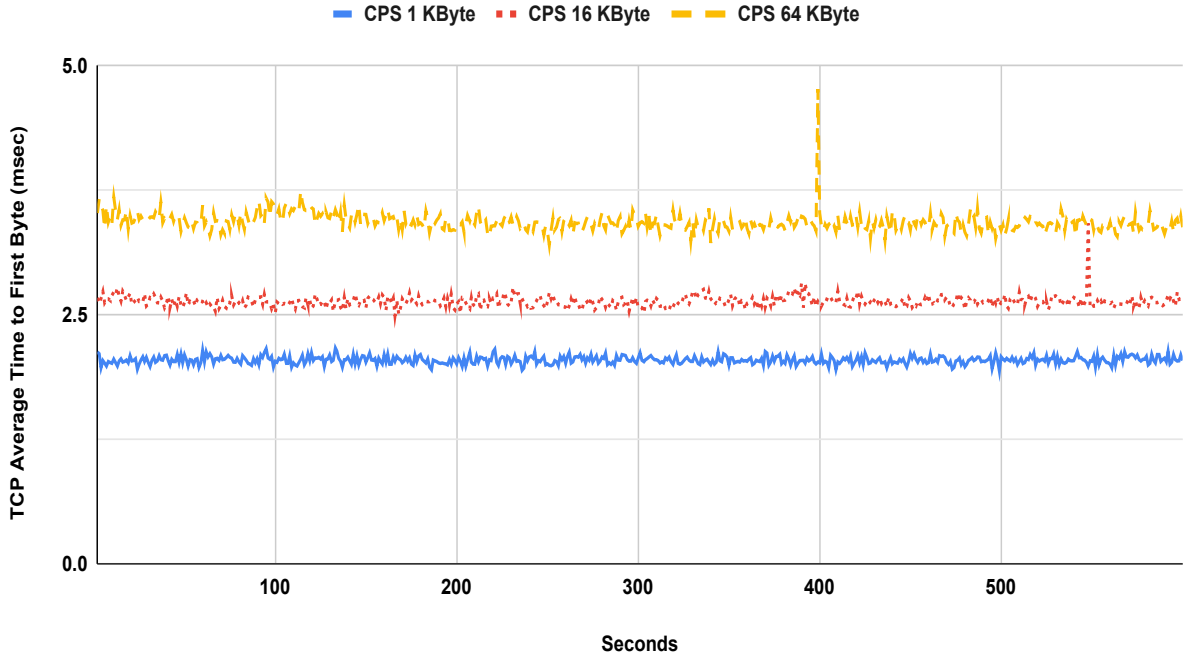


HTTPS Transactions Per Second Sustained Phase

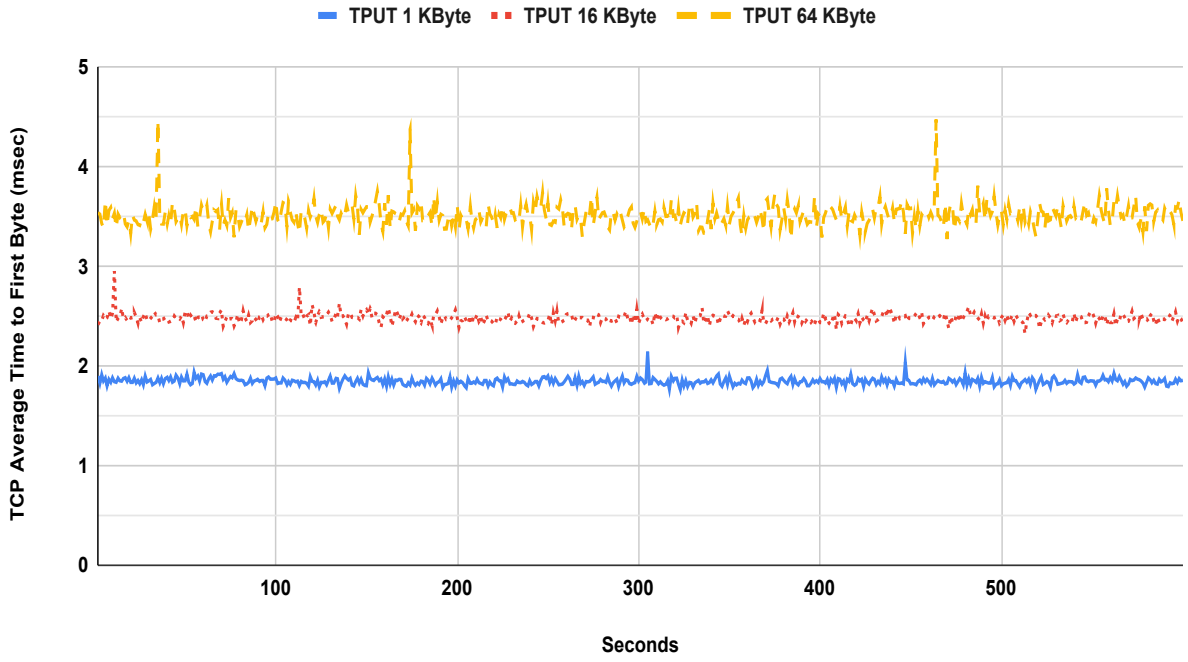


Sustainable inspected throughput of the DUT/SUT for HTTPS transactions varying the HTTPS response object size.

TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase

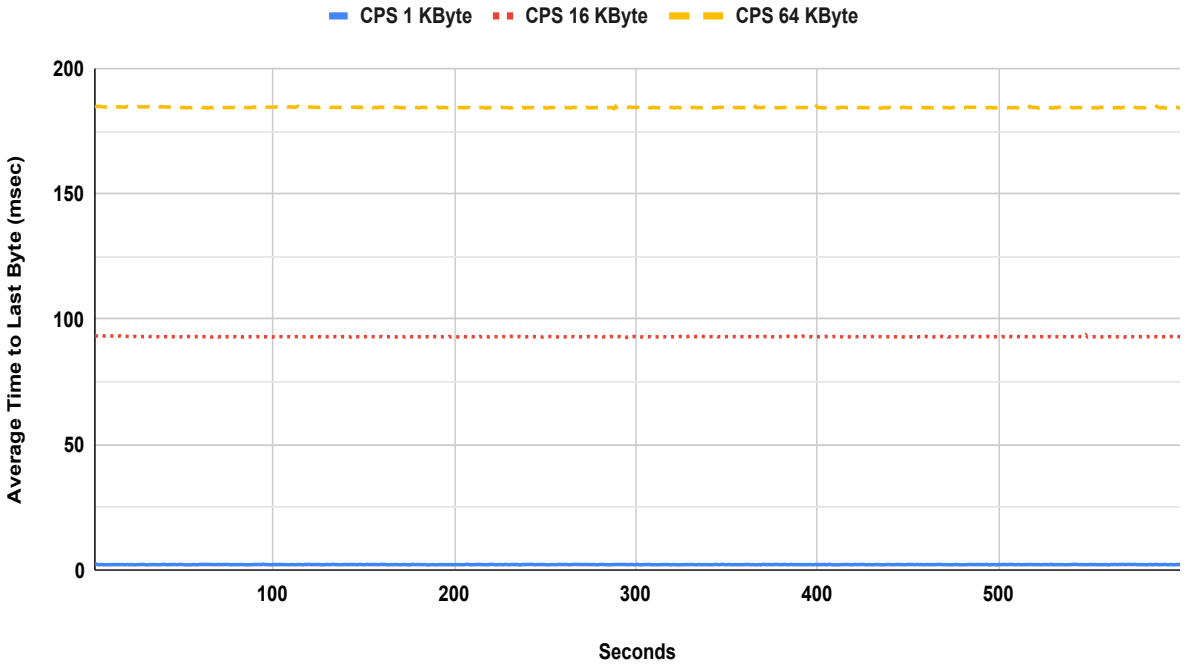


TCP/HTTPS Transaction Latency Inspected Throughput Sustained Phase

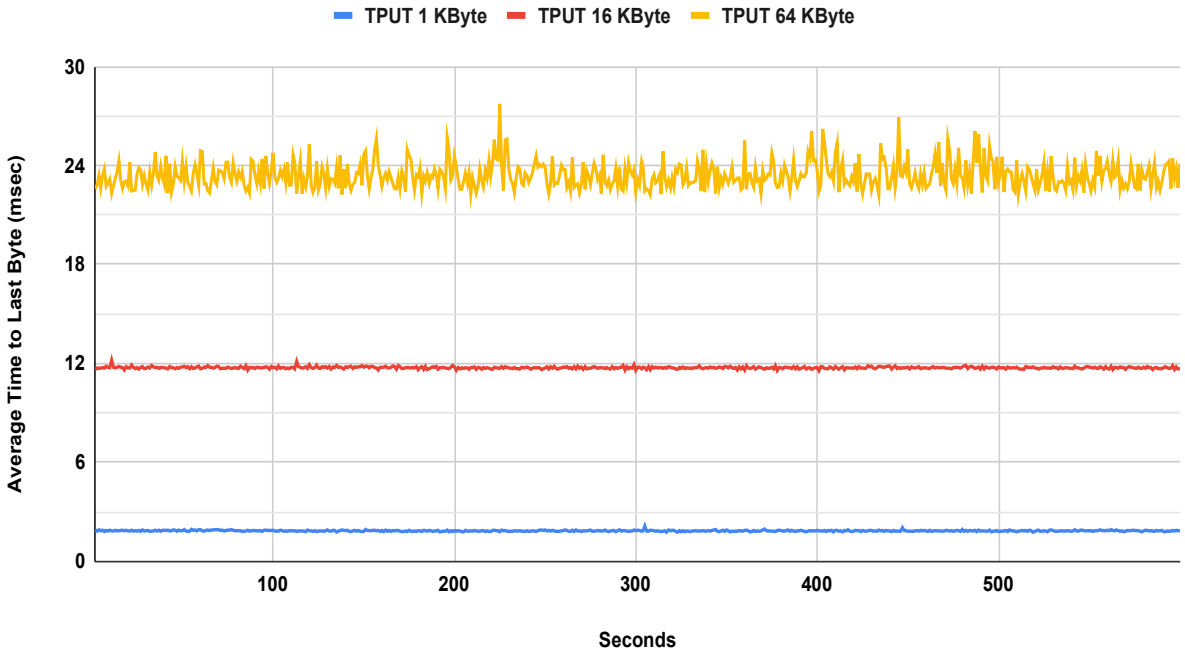


Average HTTPS transaction latency time to first byte under different HTTPS response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase

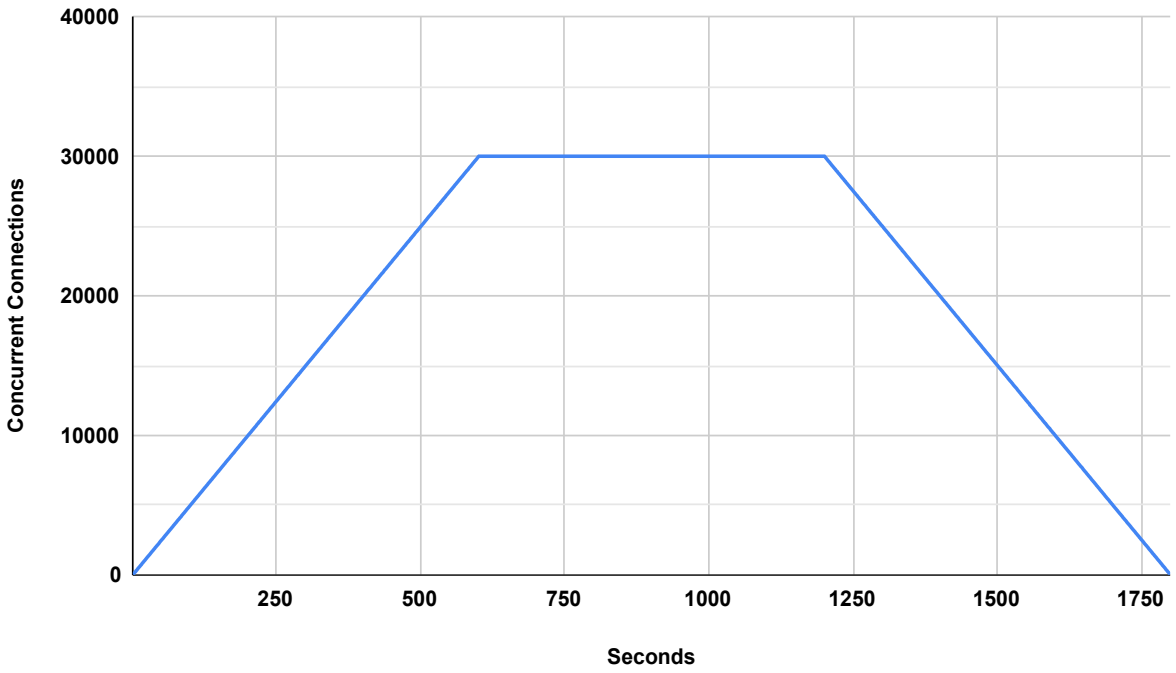


TCP/HTTPS Transaction Latency Inspected Throughput Sustained Phase



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. As described in Section 4.3.1.1, the TCP connections are initiated by clients via a TCP three-way handshake (SYN, SYN/ACK, ACK). Then, the TCP session data is sent, and then the TCP sessions are closed via either a TCP three-way close (FIN, FIN/ACK, ACK) or a TCP four-way close (FIN, ACK, FIN, ACK). The TCP sessions **MUST NOT** be closed by 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 examined and allowed traffic a network security device is able to transmit to the correct destination interface(s) in response to a specified offered load. The throughput benchmarking tests defined in Section 7 **SHOULD** measure the average layer 2 throughput value when the DUT/SUT is "inspecting" traffic. It is also acceptable to measure other OSI layer throughput. However, the measured layer (e.g., layer 3 throughput) **MUST** be noted in the report, and the user **MUST** be aware of the implication while comparing the throughput performance of multiple DUTs/SUTs measured in different OSI layers.
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 an HTTP(S) transaction, it **MUST** have a valid status code (200 OK).
TTFB	Time to First Byte	The elapsed time between the start of sending the TCP SYN packet or QUIC initial Client Hello from the client and the client receiving the first packet of application data from the server via the DUT/SUT. The benchmarking tests HTTP transaction latency (Section 7.4) and HTTPS transaction latency (Section 7.8) measure the minimum, average, and maximum

		TTFB. Minimum and maximum values are derived from the averages dataset over the sustain period. The value should be expressed in milliseconds.
TTLB	Time to Last Byte	The elapsed time between the start of sending the TCP SYN packet or QUIC initial Client Hello from the client and the client receiving the last packet of application data from the server via the DUT/SUT. The benchmarking tests HTTP transaction latency (Section 7.4) and HTTPS transaction latency (Section 7.8) measure the minimum, average, and maximum TTLB. Minimum and maximum values are derived from the averages dataset over the sustain period. The value should be expressed in milliseconds.
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]).
N/A	Not Applicable	This test does not apply to the device type or is not applicable to the testing program selected.

APPENDIX 2: SECURITY EFFECTIVENESS DETECTION RATES

This appendix focuses on validating the enabled security features of the DUT/SUT.

The public CVE set is known to the DUT/SUT vendor while the private CVE set is obscured. The CVEs are no older than 10 calendar years from the current year, selected with a focus on in-use software commonly found in business applications, and with a Common Vulnerability Scoring System (CVSS) Severity of High (7-10).

Malware definitions contain common malware types such as spyware, viruses, worms, etc. Malware samples are sent pre-infection as a payload for the DUT/SUT to detect and prevent. Command and Control (C&C) attacks post-infection are currently not included in the scenarios tested.

Evasion techniques contain CVEs previously tested in the public or private CVE sets. This is to ensure that the DUT/SUT can effectively detect and prevent the attack rather than the evasion itself. Evasions include IP fragmentation, TCP segmentation, HTML chunked segments, URL encoding, and FTP encoding.

PREVENT SCENARIO	SCENARIOS TOTAL	BLOCKED	NOT BLOCKED
Public CVE	1,381	1,360	21
Private CVE	180	178	2
Malware	3,809	3,809	0
Evasions	19	19	0

APPENDIX 3: SECURITY EFFECTIVENESS UNDER LOAD

The goal of this test is to ensure that the DUT/SUT can maintain threat detection or prevention capabilities while the inspection engine is under load with benign and malicious traffic.

Traffic mixes were leveraged with 95% of the maximum inspected throughput observed in Section 7.1.

TEST CASE	KPI	HEALTHCARE MIX			EDUCATION MIX		
Application Traffic Mix	TPUT (Mbps)	202			220		
	TPS	809			1,077		
	CVE	Scenarios total	Blocked	Not Blocked	Scenarios total	Blocked	Not Blocked
		50	50	0	50	50	0