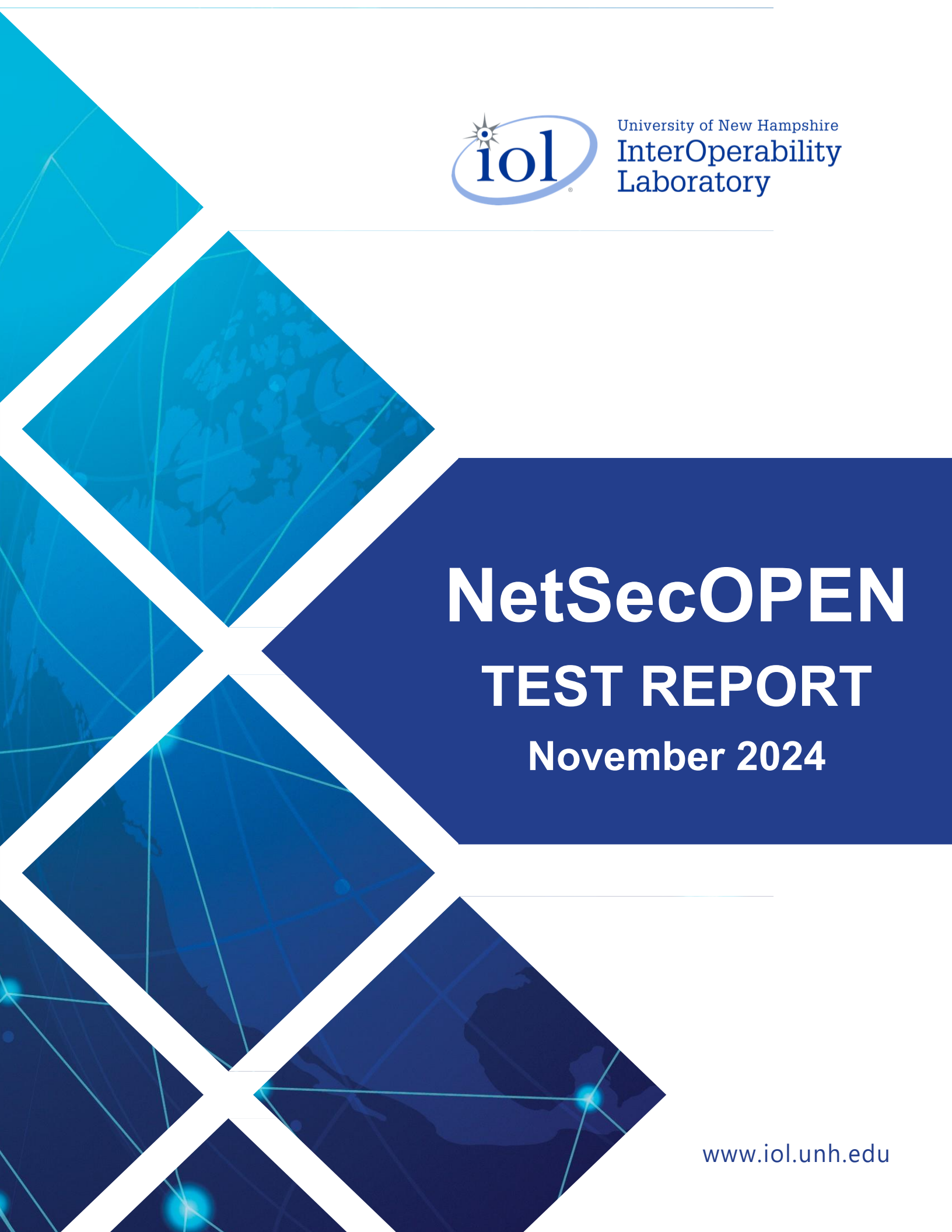


NetSecOPEN

TEST REPORT

November 2024

www.iol.unh.edu

SRAVANI SAREDDYGARI
CISCO SYSTEMS
SRSAREDD@CISCO.COM

DEVICE AND TEST PLAN INFORMATION	
Device Under Test (DUT)	C8300-2N2S-4T2X
Test Specification/Suite	Benchmarking Methodology for Network Security Device Performance RFC 9411
UNH-IOL Test Result ID	38957

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: 2024.11.18 10:03:38 -05'00'

TESTING NOTES

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

NOTES
An additional firewall rule for HTTPS traffic was created specifically for TLS-Inspection. Cisco's configuration guide for Cisco IOS XE Catalyst SD-WAN Release 17.x recommends this practice. If this rule is not created, non-encrypted traffic (HTTP) requires additional parsing. Although this is not as resource-intensive as decrypting/re-encrypting packets, it is more resource-intensive than bypassing it altogether. TLS-Inspection was enabled on the DUT/SUT for Sections 7.6 – 7.9. TLS-Inspection was disabled on the DUT/SUT for Section 7.1 and Appendix 3 pertaining to the Application Traffic Mix(s). RFC 9411 Section 7.1.3.1 permits users to disable TLS-Inspection. TLS-Inspection is the process of the DUT/SUT intercepting and decrypting inbound encrypted traffic between servers and clients. This allows for the DUT/SUT to perform content inspection on encrypted traffic. Disabling this feature can potentially cause increased performance on the DUT/SUT for test cases that include encrypted traffic.

REVISION HISTORY

The following table contains a revision history for this report.

REVISION	DATE	AUTHOR	EXPLANATION
1.0	11/13/2024	Chris Brown	Initial version
2.0	11/18/2024	Chris Brown	Updated testing notes section to include test cases where TLS-Inspection was enabled. Updated customer contact.

DEVICE INFORMATION

COMPONENT	DESCRIPTION
Device Name	C8300-2N2S-4T2X
UNH-IOL Device Identification Number	FW-CSCO-0000031142
Device Model	C8300
Software Version	Cisco IOS XE Software, Version 17.12.04
UTD Engine Version	1.1.10_SV3.1.81.0_XE17.12
UTD Signature Package Version	31810.20240912.s
AMP Module Version	1.14.6.999
Catalyst SD-WAN Manager Version	20.13.1
Splunk Enterprise Version	9.1.1
Interfaces Tested	TenGigabitEthernet0/0/4, TenGigabitEthernet0/0/5
Interfaces Speed	10G

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	11
Transport Layer	Allow	2
IP Layer	Allow	1

TEST TOOL AND ENVIRONMENT INFORMATION

COMPONENT	DESCRIPTION	
Test Equipment Vendor	Keysight	
Hardware Name	Ixia PerfectStorm One	
Hardware Firmware	10.00.1000.14	
Hardware Interface Type	10G	
Application Software Name	BreakingPoint	
Application Software Version	10.00.1.74	
Application and Threat Intelligence (ATI) Strikepack Version	2024-13	
Application Software Name	BreakingPoint QuickTest	
Application Software Version	10.00.10.47	
Client IP Subnet	10.45.0.0/23	
Server IP Subnet	10.46.0.0/23	
Traffic Distribution Ratio	**IPv4**	**IPv6**
	100%	0%
Cipher Suite	ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048	

TESTBED SETUP

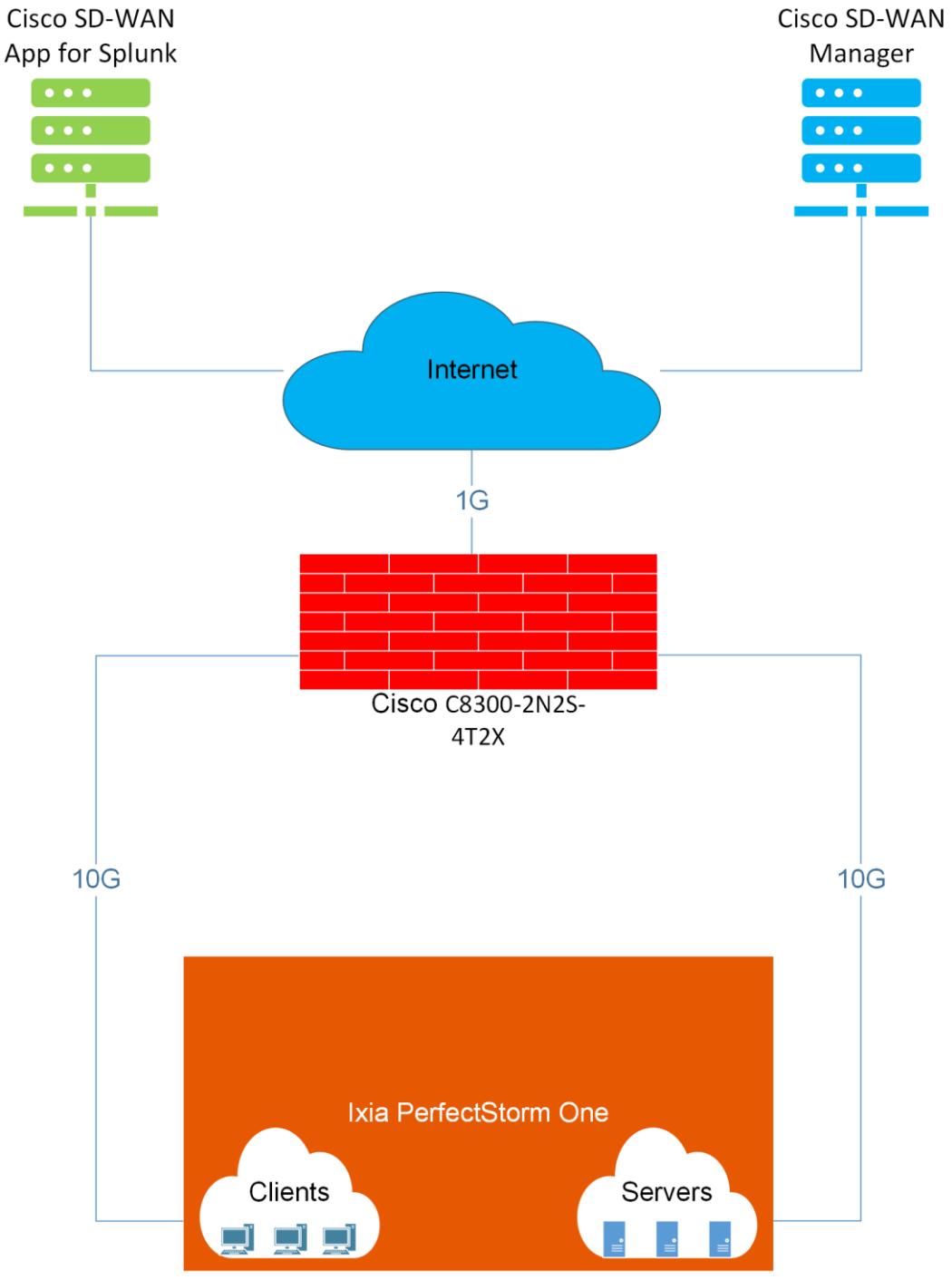


Figure 1: Topology with Test Equipment Vendor

SECURITY EFFECTIVENESS SUMMARY

SCENARIO	TOTAL	BLOCKED	ALLOWED	BLOCK RATE
Public CVE	1,380	1,349	31	97.75%
Private CVE	180	178	2	98.88%
Malware	3,809	3,779	30	99.21%
Evasions	19	19	0	100%
More information can be found at APPENDIX 2				

SECURITY TESTING UNDER LOAD		
Traffic Mix Type:	Healthcare	Education
TPUT Gbps (Kbps)	3.22 (3,220,000)	2.74 (2,741,000)
TPS	13,189	14,708
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 Gbps (Kbps)	3.42 (3,421,000)	2.91 (2,907,000)
	TPS	14,115	15,670

SECTION 7.2

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTP Connections Per Second	CPS	18,069	16,784	15,276	8,523	4,549

SECTION 7.3

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTP Inspected Throughput	TPUT Gbps (Kbps)	0.46 (465,000)	1.60 (1,598,000)	2.77 (2,769,000)	3.70 (3,699,000)	2.78 (2,784,000)
	TPS	27,876	11,141	5,019	1,691	6,125

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)	1.107	1.301	1.589	2.008	3.398	3.203
	TTFB Minimum (msec)	0.941	1.199	1.348	1.934	3.256	3.063
	TTFB Maximum (msec)	1.283	1.422	1.768	2.122	3.555	3.306
	TTLB Average (msec)	1.116	1.416	1.696	2.986	5.904	5.553
	TTLB Minimum (msec)	0.953	1.332	1.470	2.899	5.810	5.470
	TTLB Maximum (msec)	1.293	1.542	1.869	3.137	5.994	5.642

SECTION 7.5

TEST CASE	KPI	1K
Concurrent TCP/HTTP Connection Capacity	CC	219,000

SECTION 7.6

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTPS Connections Per Second	CPS	129	130	131	128	125
	HR	1K				
		129				

SECTION 7.7

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTPS Inspected Throughput	TPUT Gbps (Kbps)	0.02 (22,000)	0.18 (179,000)	0.38 (382,000)	0.24 (243,000)	0.39 (387,000)
	TPS	1,294	1,225	685	110	843

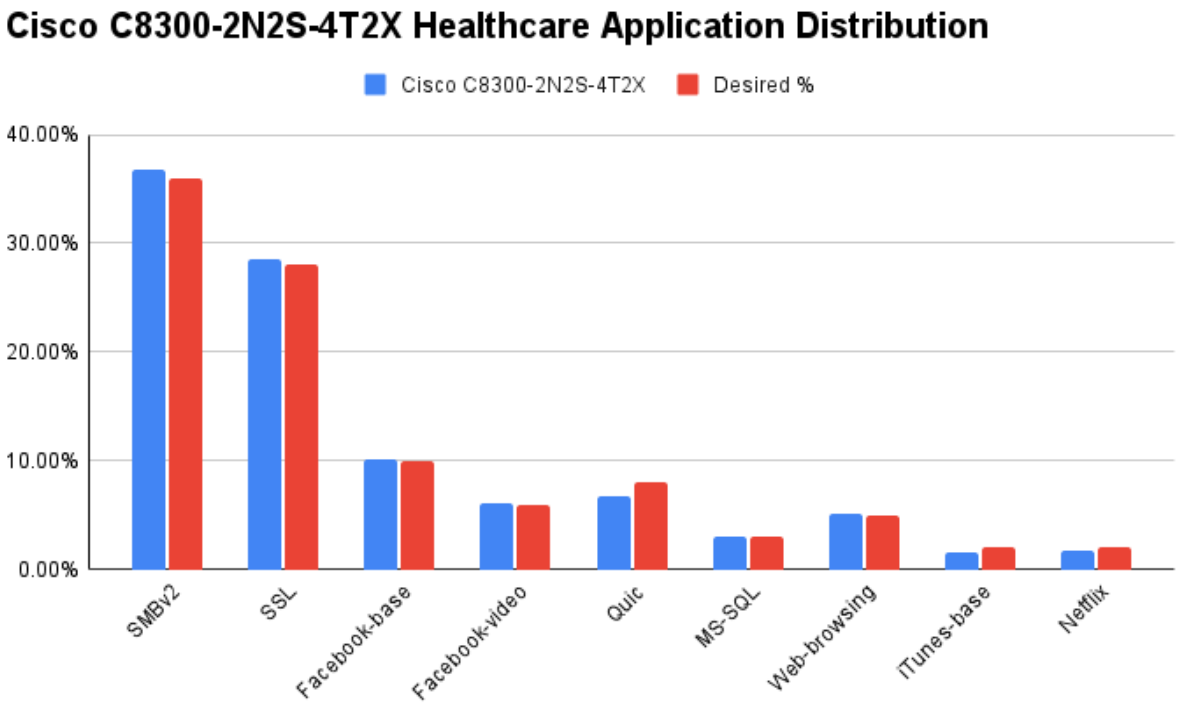
SECTION 7.8

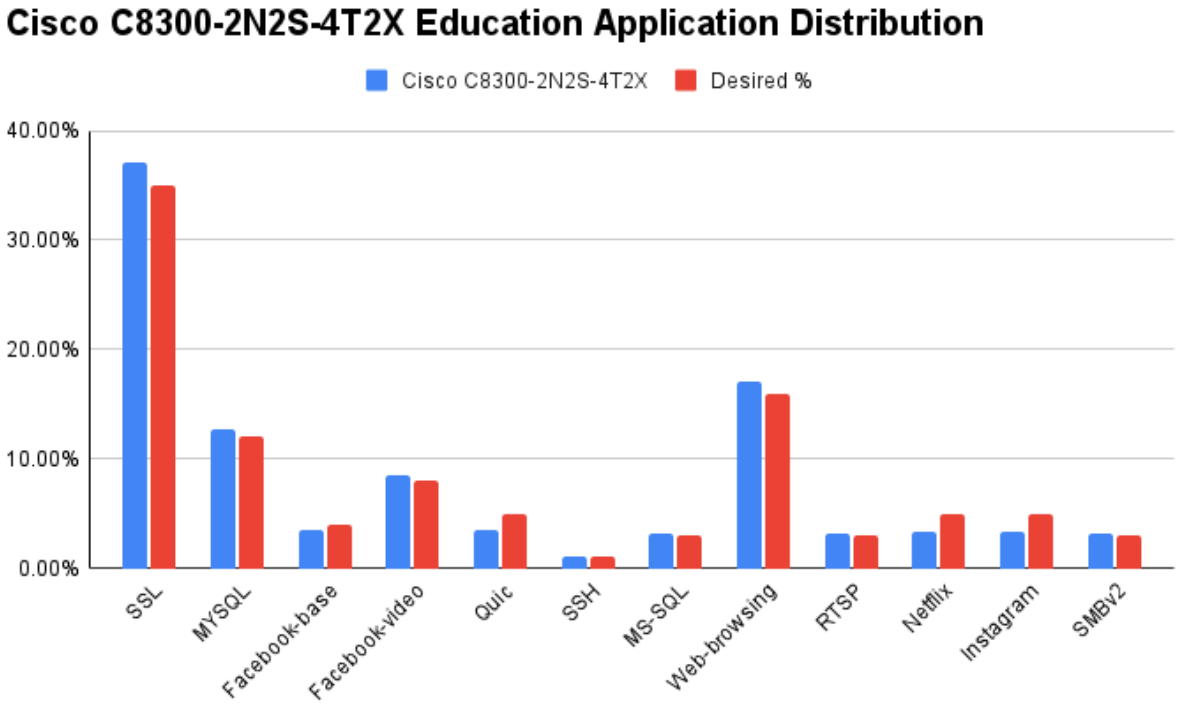
TEST CASE	KPI	CPS 1K	CPS 16K	CPS 64K	TPUT 1K	TPUT 16K	TPUT 64K
TCP/HTTPS Transaction Latency	TTFB Average (msec)	0.926	1.089	1.369	7.176	18.151	36.319
	TTFB Minimum (msec)	0.741	0.921	1.145	6.689	16.432	26.149
	TTFB Maximum (msec)	1.158	1.437	1.645	7.661	19.268	47.651
	TTLB Average (msec)	0.935	2.091	68.024	7.174	19.271	290.181
	TTLB Minimum (msec)	0.741	1.861	63.672	6.687	17.992	276.408
	TTLB Maximum (msec)	1.174	2.476	74.753	7.661	19.942	303.223

SECTION 7.9

TEST CASE	KPI	1K
Concurrent TCP/HTTPS Connection Capacity	CC	39,988

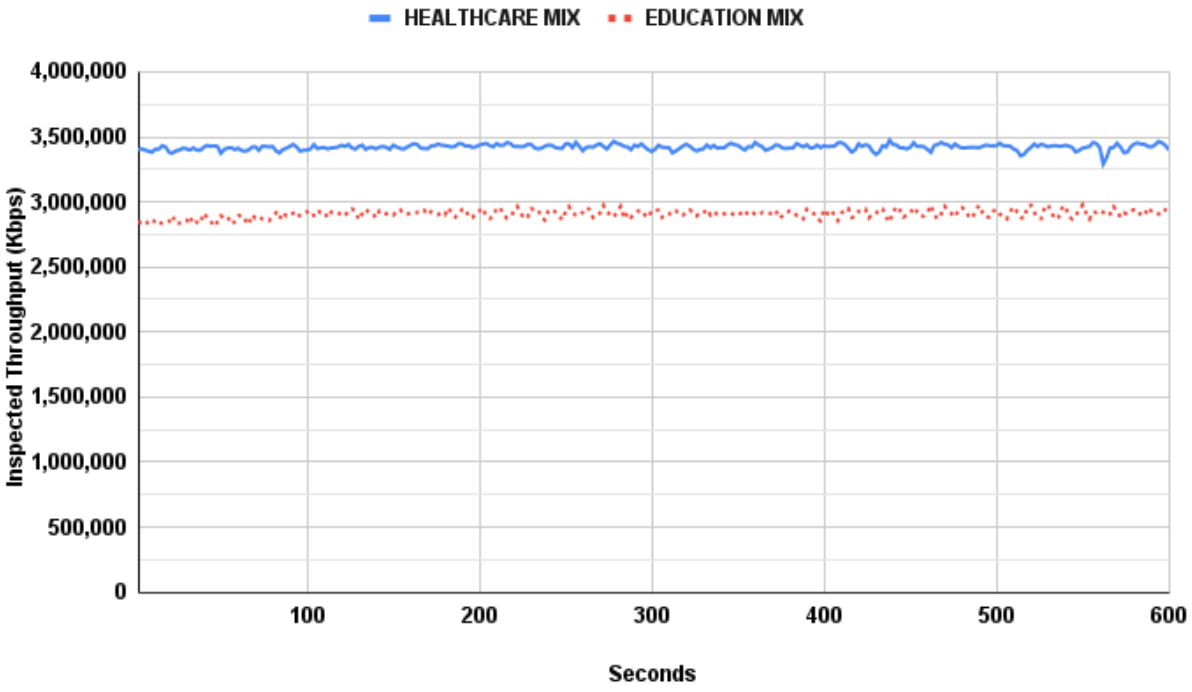
GRAPHS



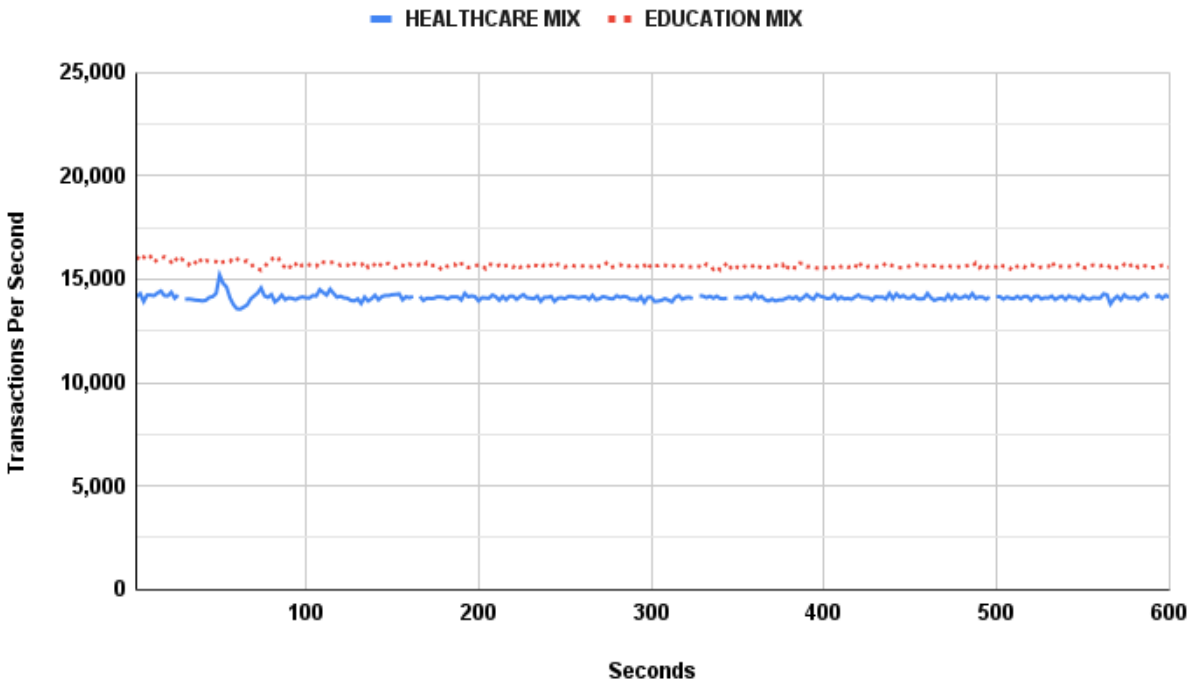


Comparison of desired Inspected Throughput and observed Inspected Throughput for each application within the traffic mixes.

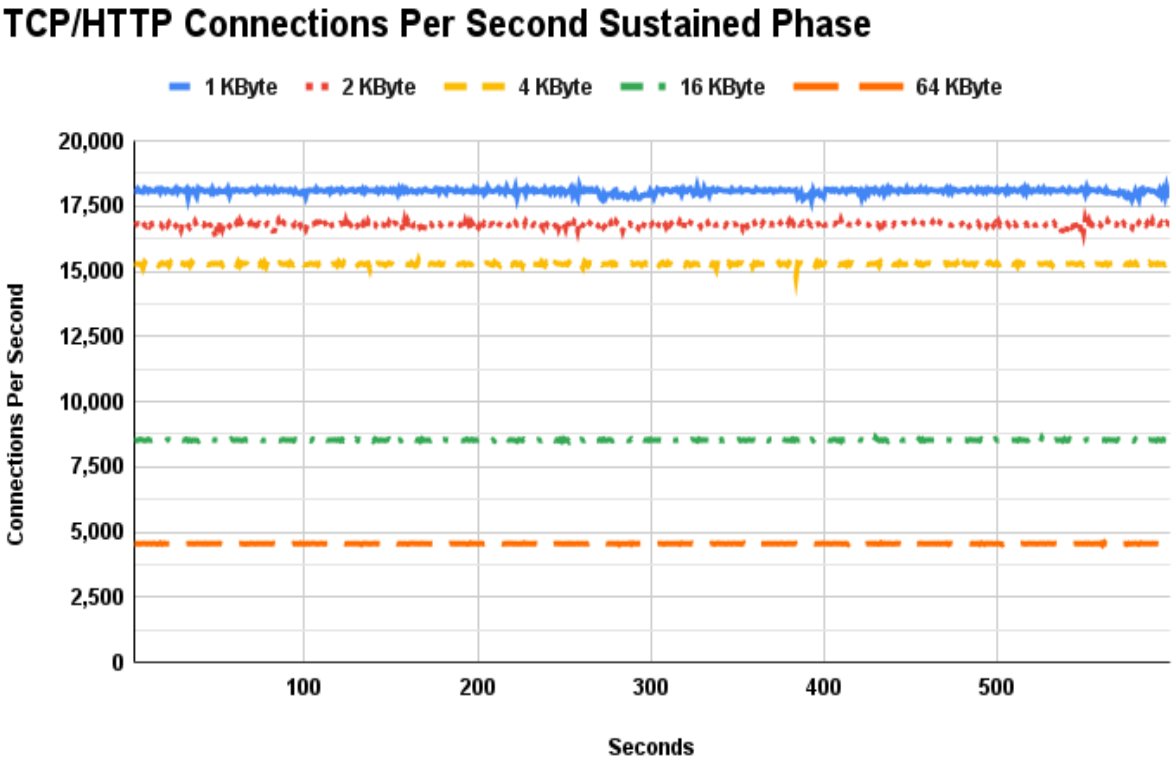
Inspected Throughput Sustained Phase



Transactions Per Second Sustained Phase

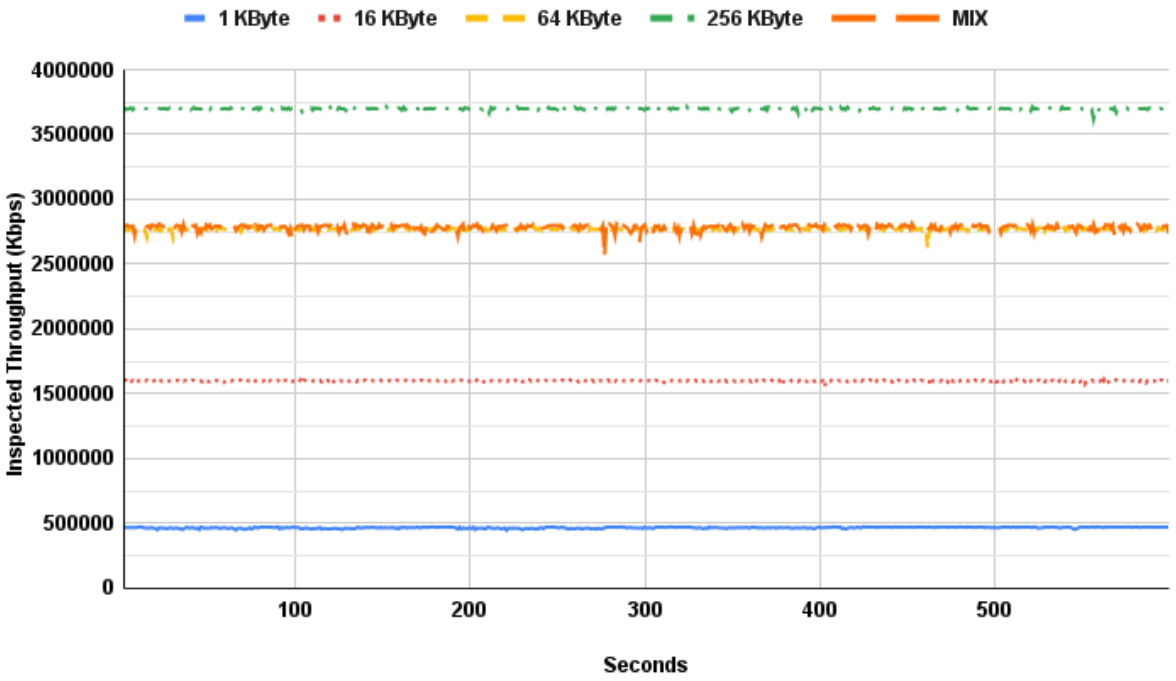


Sustainable inspected throughput of the DUT/SUT for Application Traffic Mixes.

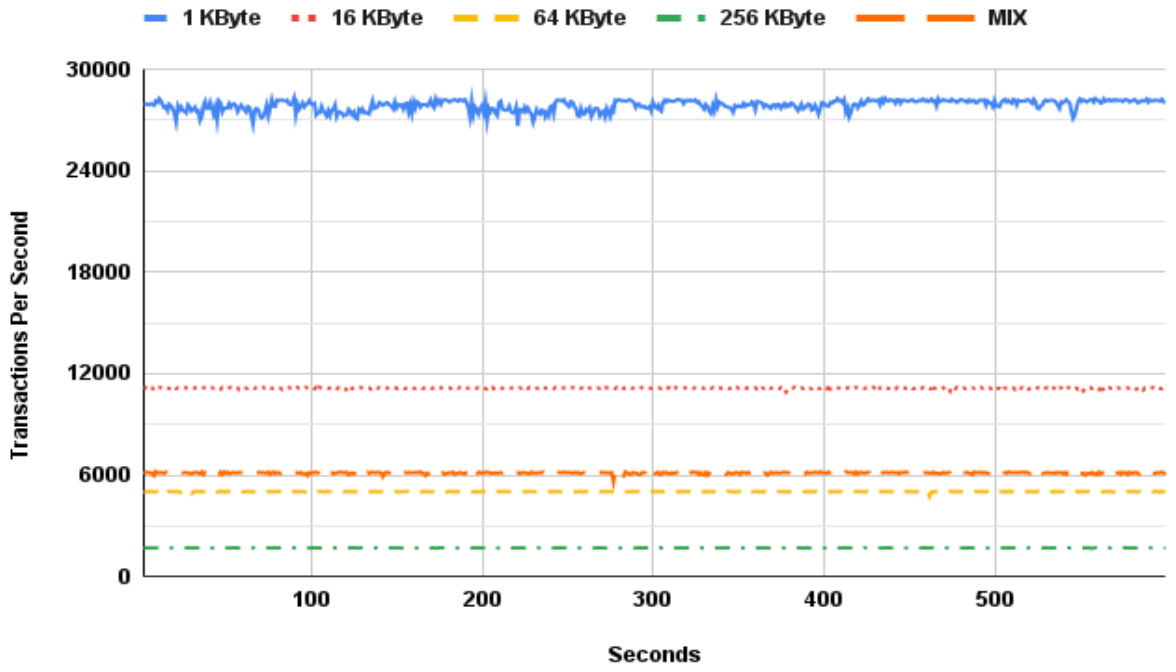


Sustainable TCP/HTTP connection establishment rate supported by the DUT/SUT under different throughput load conditions.

HTTP Inspected Throughput Sustained Phase

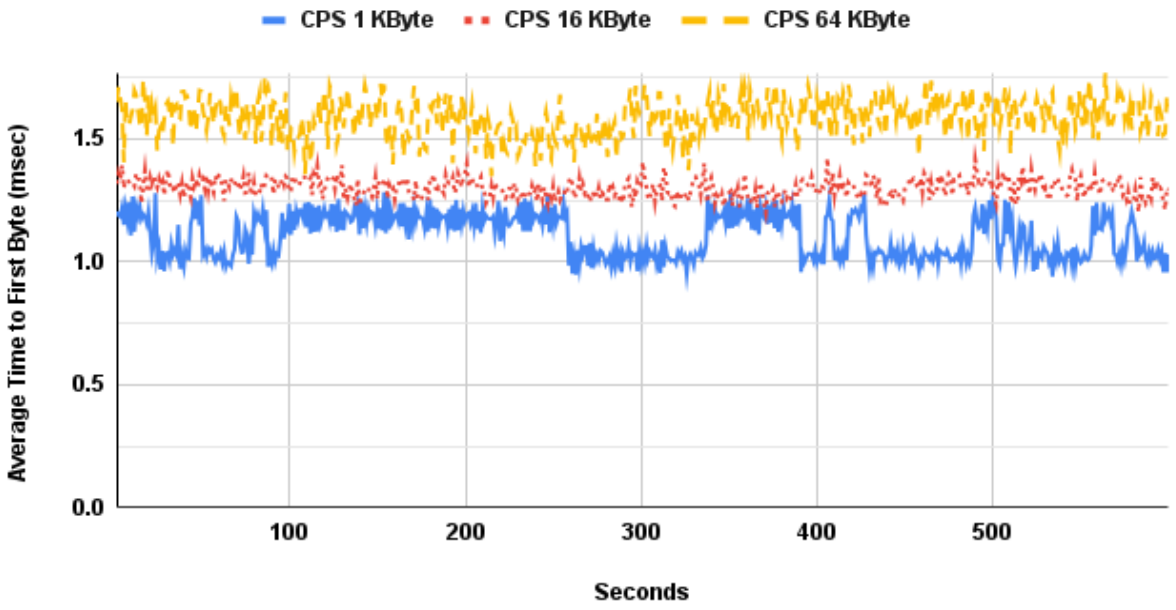


HTTP Transactions Per Second Sustained Phase

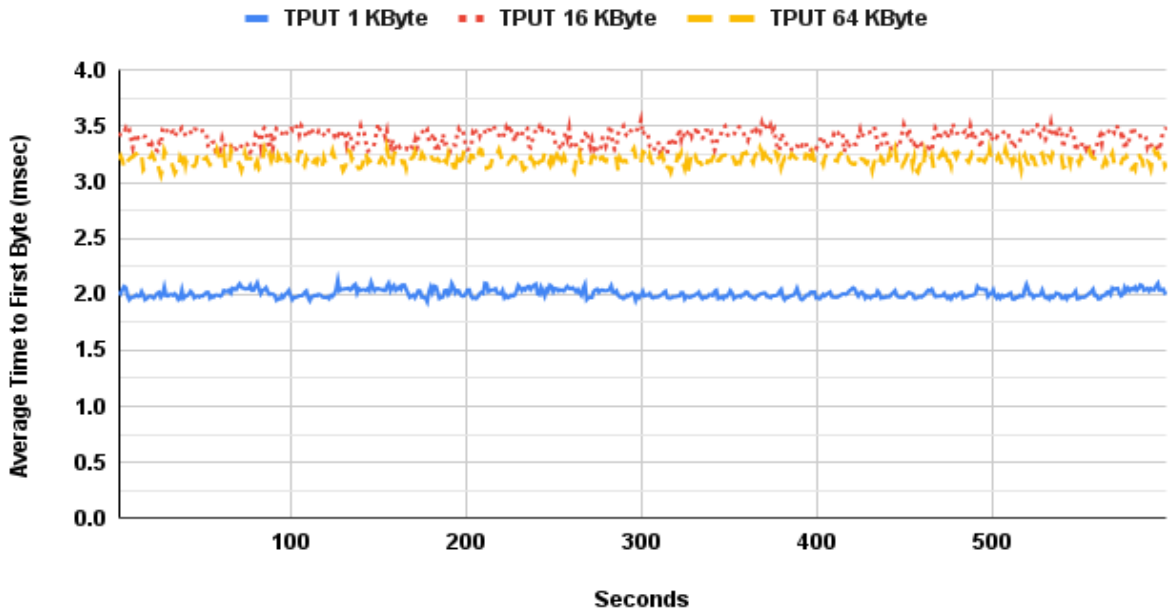


Sustainable inspected throughput of the DUT/SUT for HTTP transactions varying the HTTP response object size.

TCP/HTTP Transaction Latency Connections Per Second Sustained Phase

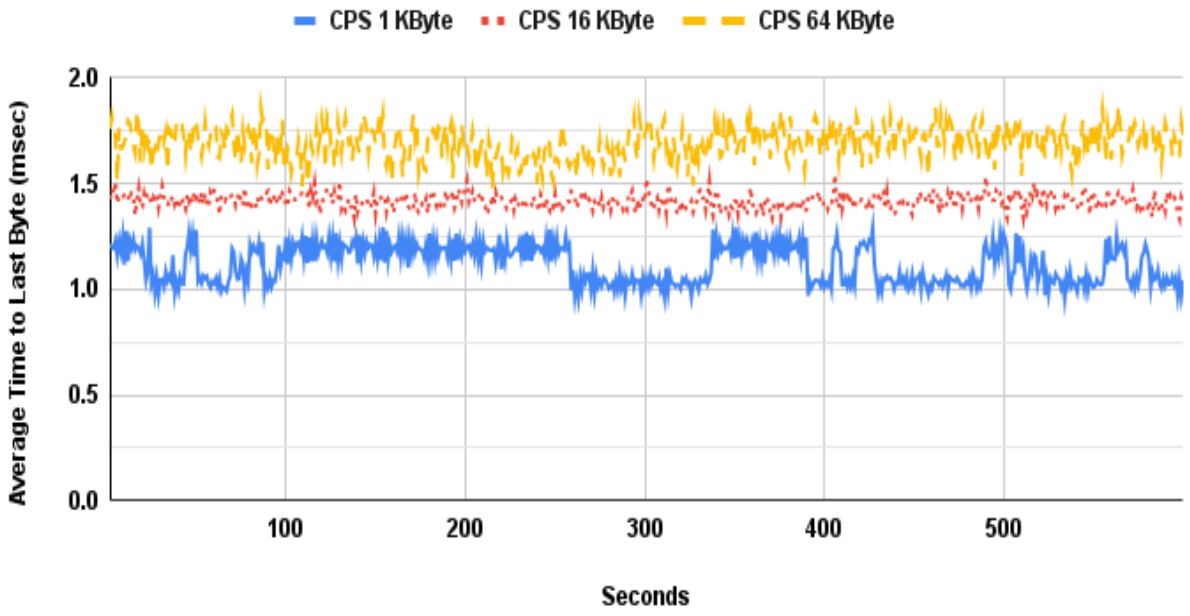


TCP/HTTP Transaction Latency Inspected Throughput Sustained Phase

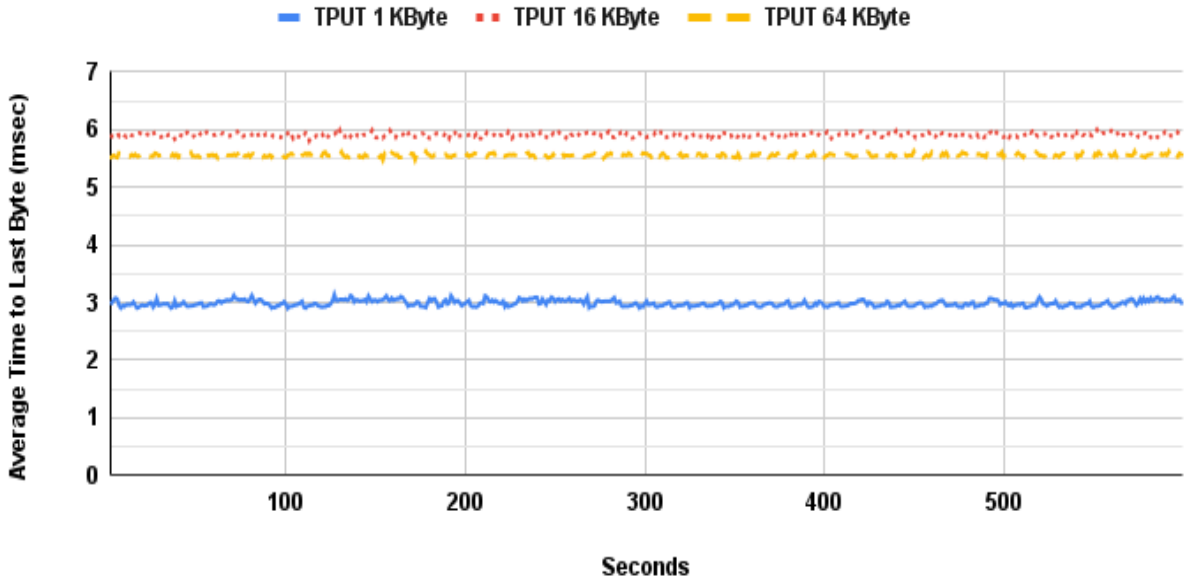


Average HTTP transaction latency time to first byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

TCP/HTTP Transaction Latency Connections Per Second Sustained Phase

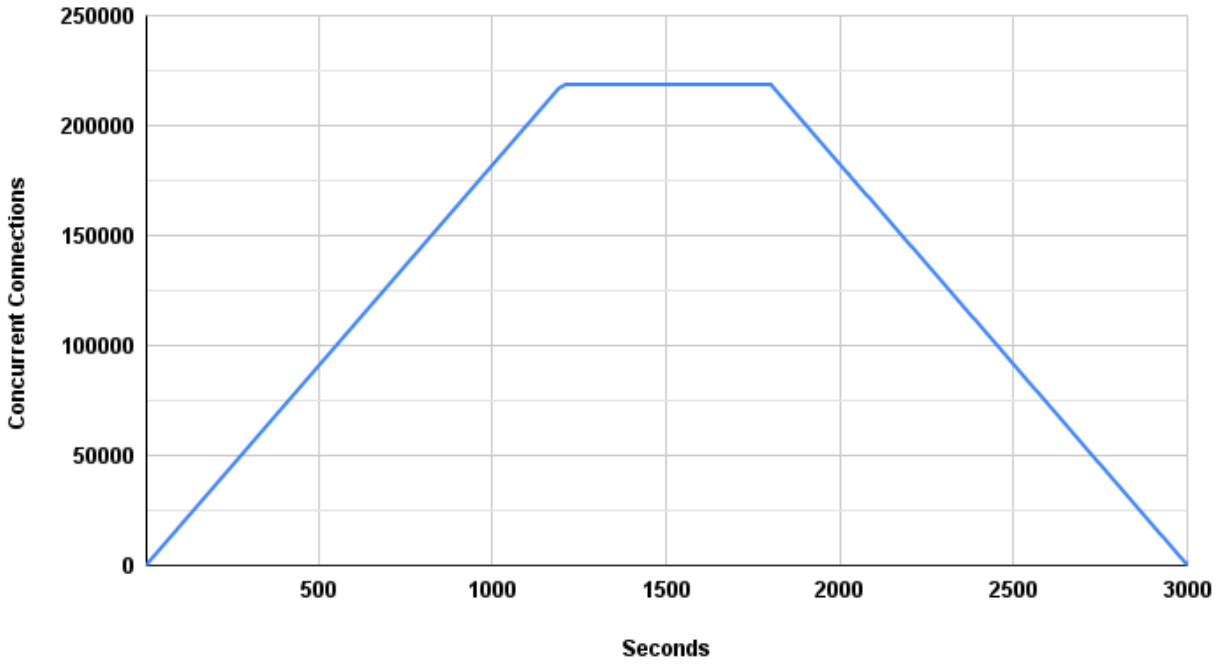


TCP/HTTP Transaction Latency Inspected Throughput Sustained Phase



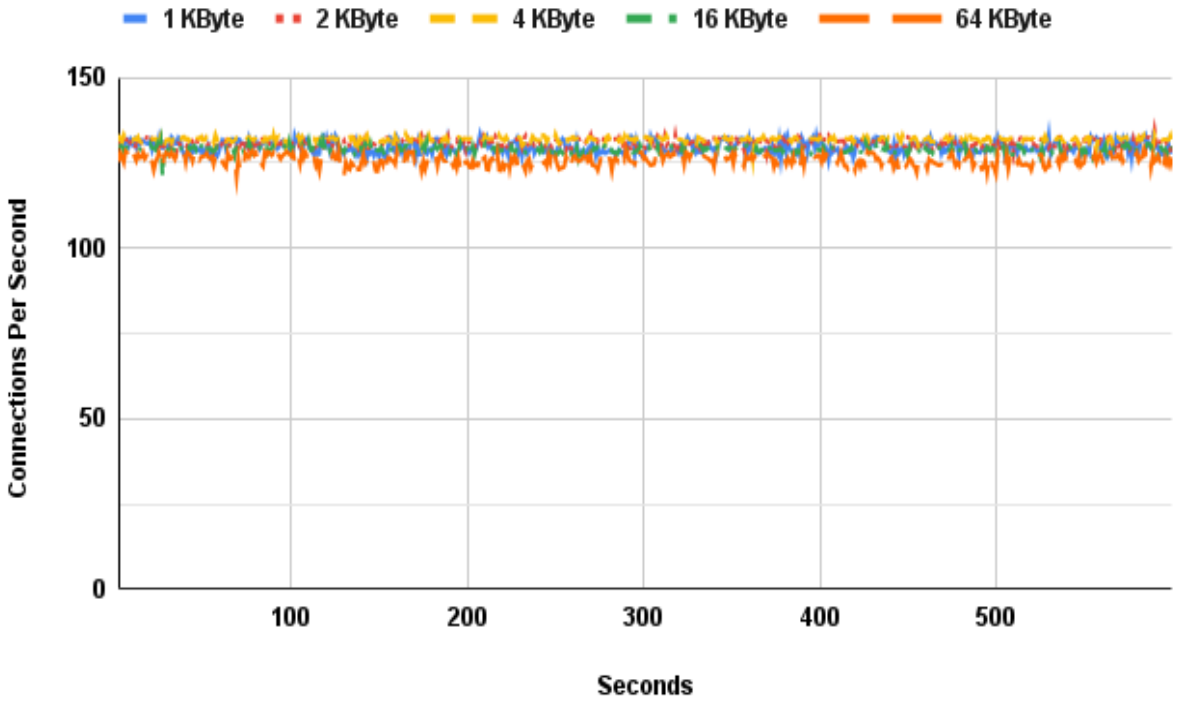
Average HTTP transaction latency time to last byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

Concurrent TCP/HTTP Connection Capacity

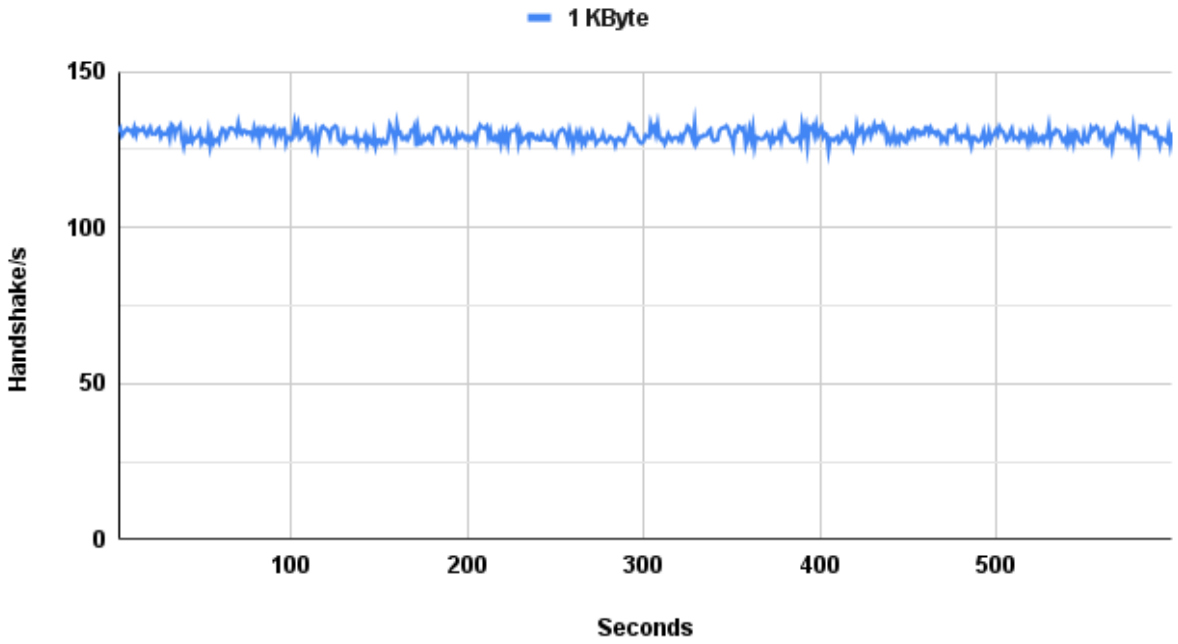


Number of concurrent TCP connections that the DUT/SUT sustains when using HTTP traffic.

TCP/HTTPS Connections Per Second Sustained Phase

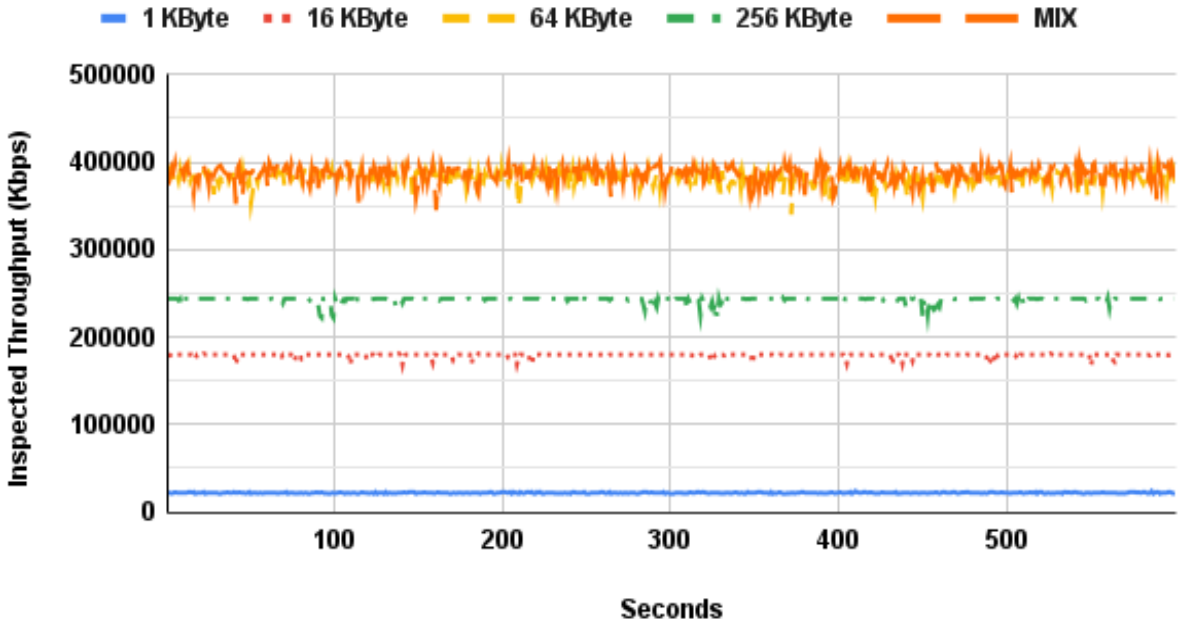


TCP/HTTPS TLS Handshake Rate Sustained Phase

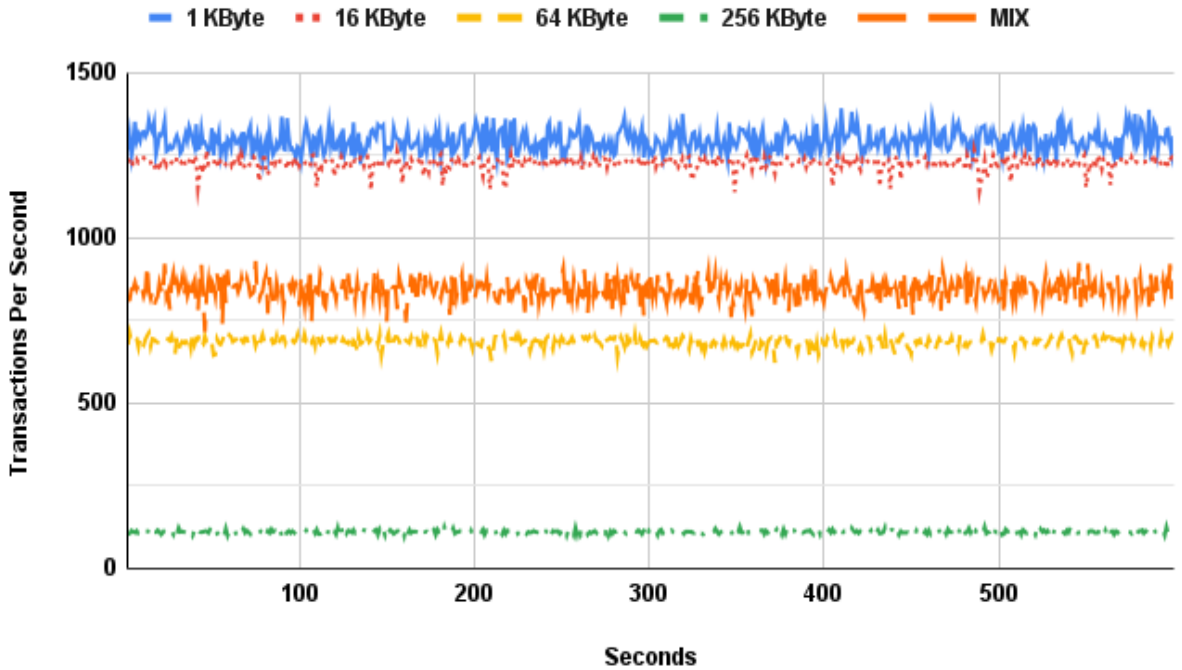


Sustainable SSL/TLS session establishment rate supported by the DUT/SUT under different throughput load conditions.

HTTPS Inspected Throughput Sustained Phase

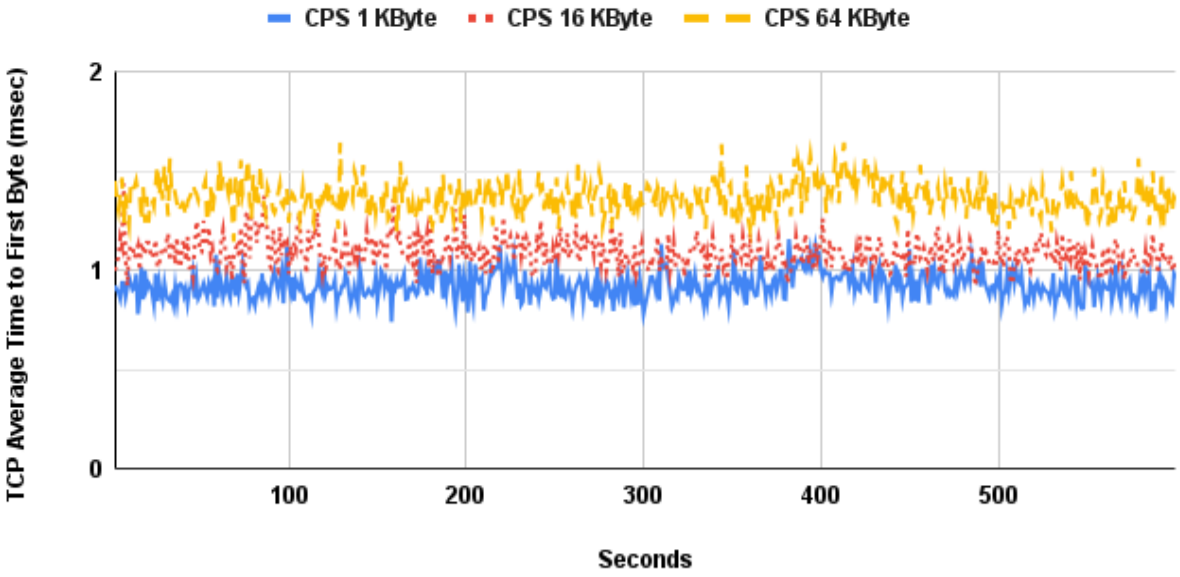


HTTPS Transactions Per Second Sustained Phase

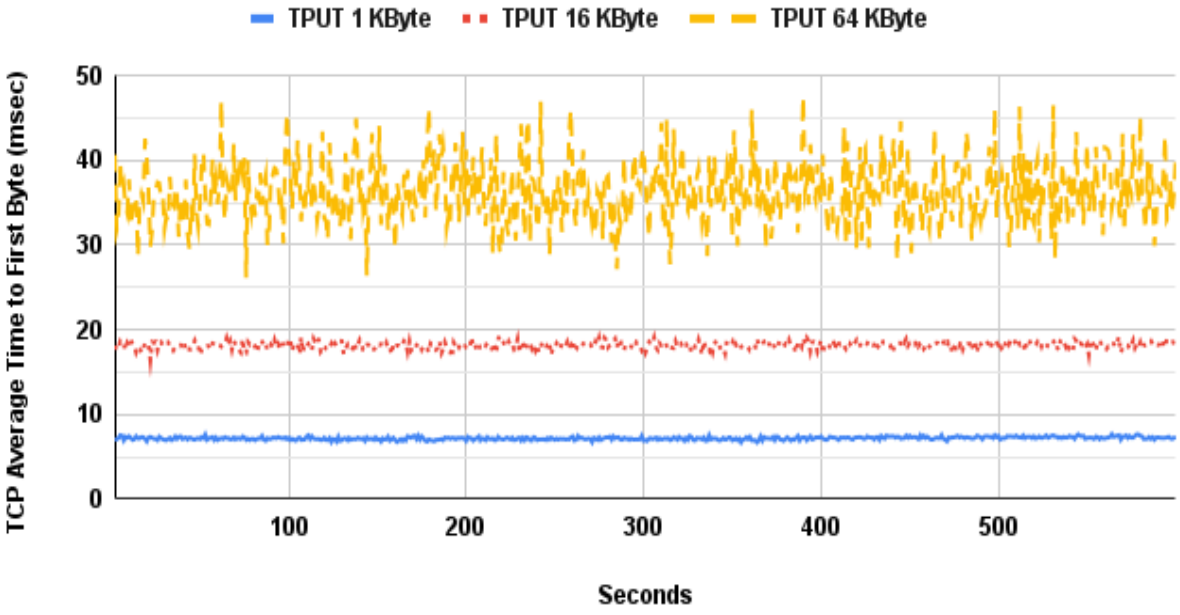


Sustainable inspected throughput of the DUT/SUT for HTTPS transactions varying the HTTPS response object size.

TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase

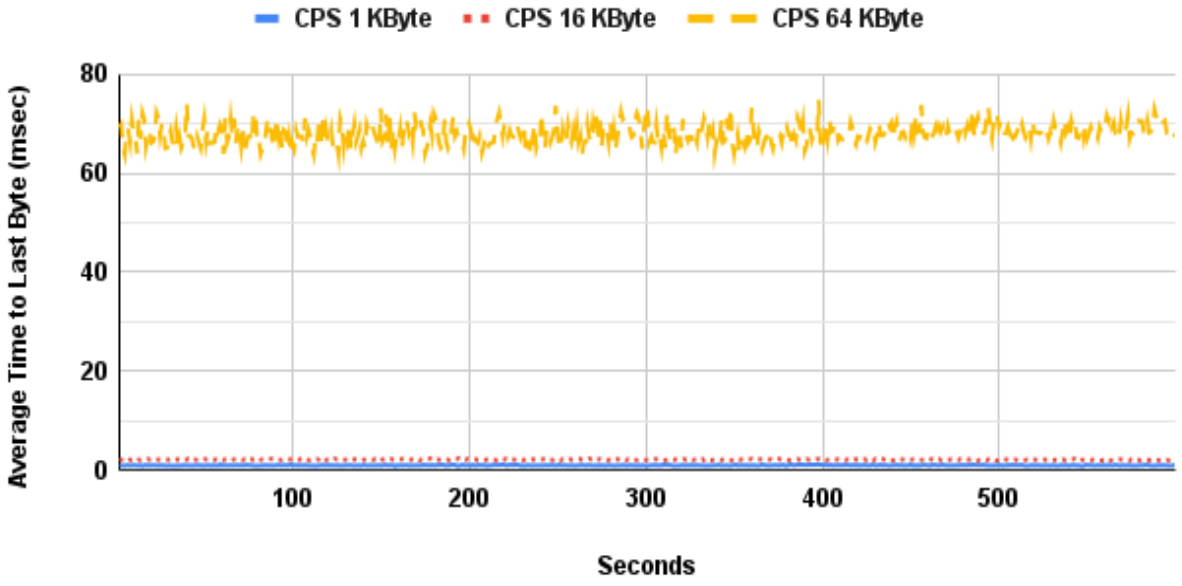


TCP/HTTPS Transaction Latency Inspected Throughput Sustained Phase

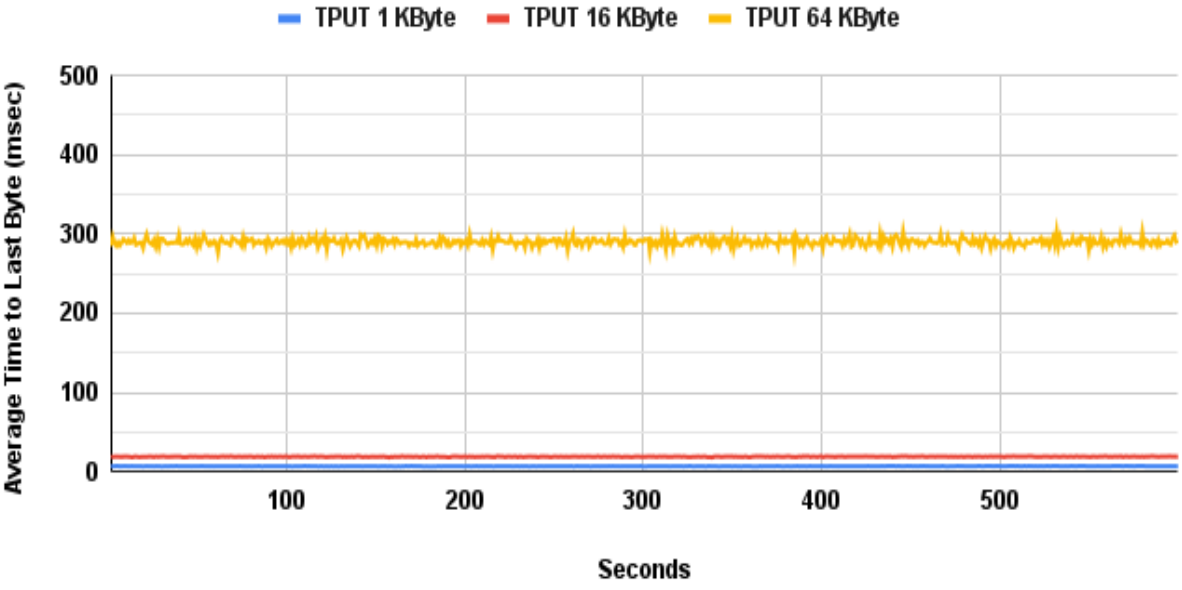


Average HTTPS transaction latency time to first byte under different HTTPS response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

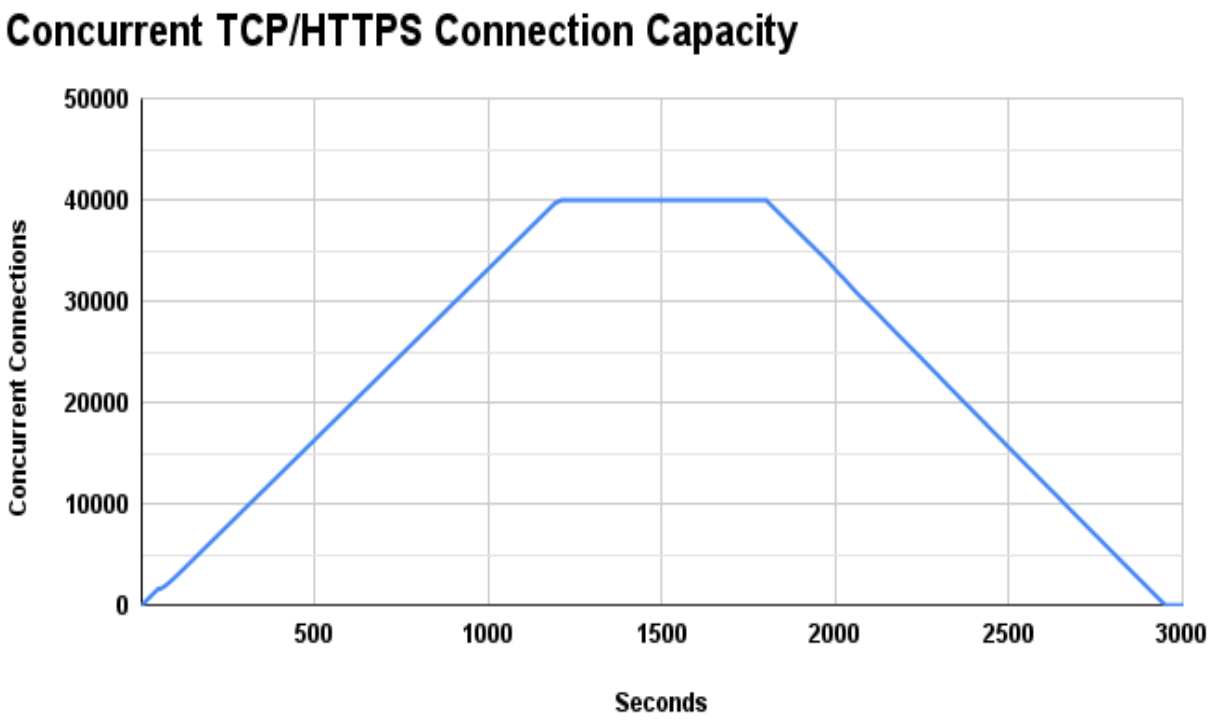
TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase



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.



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	1,380	1,349	31
Private CVE	180	178	2
Malware	3,809	3,779	30
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. CVE traffic transmission rate is set to 10 CVEs per second.

TEST CASE	KPI	HEALTHCARE MIX				EDUCATION MIX			
Application Traffic Mix	TPUT Gbps (Kbps)	3.22 (3,220,000)				2.74 (2,741,000)			
	TPS	13,189				14,708			
	CVE	Unique CVEs	Scenarios total	Blocked	Not Blocked	Unique CVEs	Scenarios total	Blocked	Not Blocked
		50	900	900	0	50	900	900	0