



University of New Hampshire
InterOperability
Laboratory

NetSecOPEN

TEST REPORT

September 2024

www.iol.unh.edu

AKBAL SINGH KARLCUT
 SONICWALL INC.
AKARLCUT@SONICWALL.COM

DEVICE AND TEST PLAN INFORMATION

Device Under Test (DUT)	SonicWall NSa 4700
Test Specification/Suite	Benchmarking Methodology for Network Security Device Performance RFC 9411
UNH-IOL Test Result ID	38606

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.

TESTING NOTES

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

NOTES
No unusual device activity was observed during this testing.

REVISION HISTORY

The following table contains a revision history for this report.

REVISION	DATE	AUTHOR	EXPLANATION
1.0	09/30/2024	Chris Brown	Initial version
2.0	11/01/2024	Chris Brown	Updated Appendix 2 with correct Evasion numbers

DEVICE INFORMATION

COMPONENT	DESCRIPTION
Device Name	SonicWall NSa 4700
UNH-IOL Device Identification Number	FW-SONICW-0000030872
Device Model	4700
Software Version	SonicOS 7.0.1-6009
ROM Version	15.0.0.0
Gateway Anti-Virus Signature Database Timestamp	UTC 09/06/2024 14:14:05.000
Anti-Spyware Signature Database Timestamp	UTC 09/06/2024 12:36:16.000
Intrusion Prevention Signature Database Timestamp	UTC 09/06/2024 15:32:03.000
Interfaces Tested	X24, X25
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	20
Transport Layer	Block	100
IP Layer	Block	100
Application Layer	Allow	10
Transport Layer	Allow	3
IP Layer	Allow	1

TEST TOOL AND ENVIRONMENT INFORMATION

COMPONENT	DESCRIPTION	
Test Equipment Vendor	Spirent	
Hardware Name	SPT-C100-S3	
Hardware Firmware	5.47.3813	
Hardware Interface Type	10G	
Application Software Name	Cyberflood	
Application Software Version	24.3.1012	
Client IP Subnet	10.10.0.0/23	
Server IP Subnet	10.11.0.0/23	
Traffic Distribution Ratio	IPv4	IPv6
	100%	0%
Cipher Suite	ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048	

TESTBED SETUP

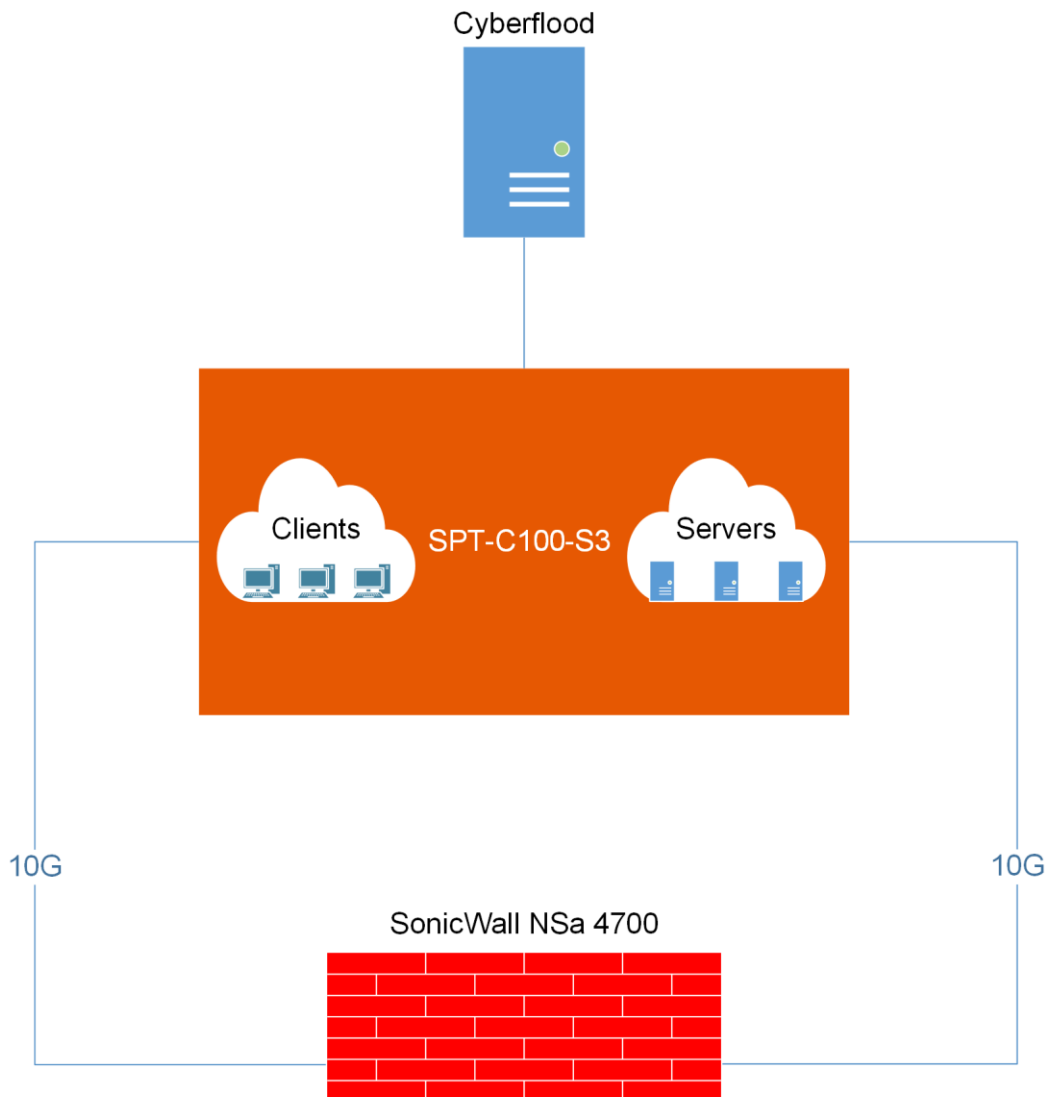


Figure 1: Topology with Test Equipment Vendor

SECURITY EFFECTIVENESS SUMMARY

SCENARIO	TOTAL	BLOCKED	ALLOWED	BLOCK RATE
Public CVE	1,380	1380	0	100.00%
Private CVE	180	180	0	100.00%
Malware	3,809	3809	0	100.00%
Evasions	19	19	0	100.00%

More information can be found at [APPENDIX 2](#)

SECURITY TESTING UNDER LOAD		
Traffic Mix Type:	Healthcare	Education
TPUT Gbps (Kbps)	0.91 (912,733)	0.76 (763,233)
TPS	3,084	2,738
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)	0.96 (958,001)	0.83 (827,095)
	TPS	2,862	3,030

SECTION 7.2

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTP Connections Per Second	CPS	30,510	22,180	14,982	5,324	1,661

SECTION 7.3

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTP Inspected Throughput	TPUT Gbps (Kbps)	1.29 (1,293,281)	3.94 (3,938,212)	5.26 (5,257,698)	6.52 (6,520,771)	5.69 (5,693,940)
	TPS	112,203	28,715	9,773	3,043	12,874

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)	0.466	0.593	0.934	0.488	0.620	0.820
	TTFB Minimum (msec)	0.461	0.575	0.824	0.482	0.601	0.742
	TTFB Maximum (msec)	0.471	0.612	1.045	0.504	0.666	0.918
	TTLB Average (msec)	0.301	1.341	4.122	0.185	0.355	0.780
	TTLB Minimum (msec)	0.299	1.317	4.072	0.184	0.349	0.760
	TTLB Maximum (msec)	0.306	1.359	4.197	0.187	0.366	0.802

SECTION 7.5

TEST CASE	KPI	1K
Concurrent TCP/HTTP Connection Capacity	CC	1,996,511



SECTION 7.6

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTPS Connections Per Second	CPS	2,200	2,170	2,169	2,017	1,565
	HR	1K				

SECTION 7.7

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTPS Inspected Throughput	TPUT	0.30	1.67	2.82	3.29	2.62
	Gbps (Kbps)	(295,637)	(1,670,529)	(2,819,760)	(3,288,839)	(2,618,949)
	TPS	19,558	11,869	5,168	1,520	5,822



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)	5.356	5.258	5.460	5.140	5.031	5.071
	TTFB Minimum (msec)	5.224	5.156	5.163	5.074	4.958	4.963
	TTFB Maximum (msec)	5.555	5.653	6.287	5.303	5.109	5.341
	TTLB Average (msec)	0.331	0.467	1.334	0.213	0.369	0.858
	TTLB Minimum (msec)	0.282	0.430	1.142	0.206	0.360	0.826
	TTLB Maximum (msec)	0.431	0.537	2.196	0.226	0.391	0.913

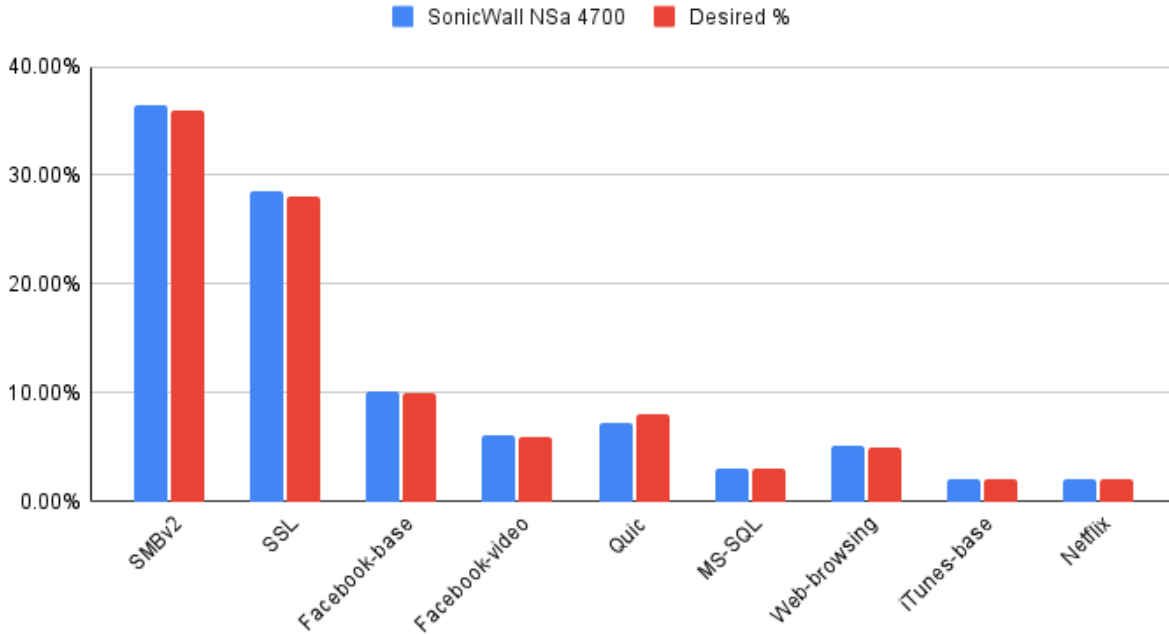
SECTION 7.9

TEST CASE	KPI	1K
Concurrent TCP/HTTPS Connection Capacity	CC	278,172

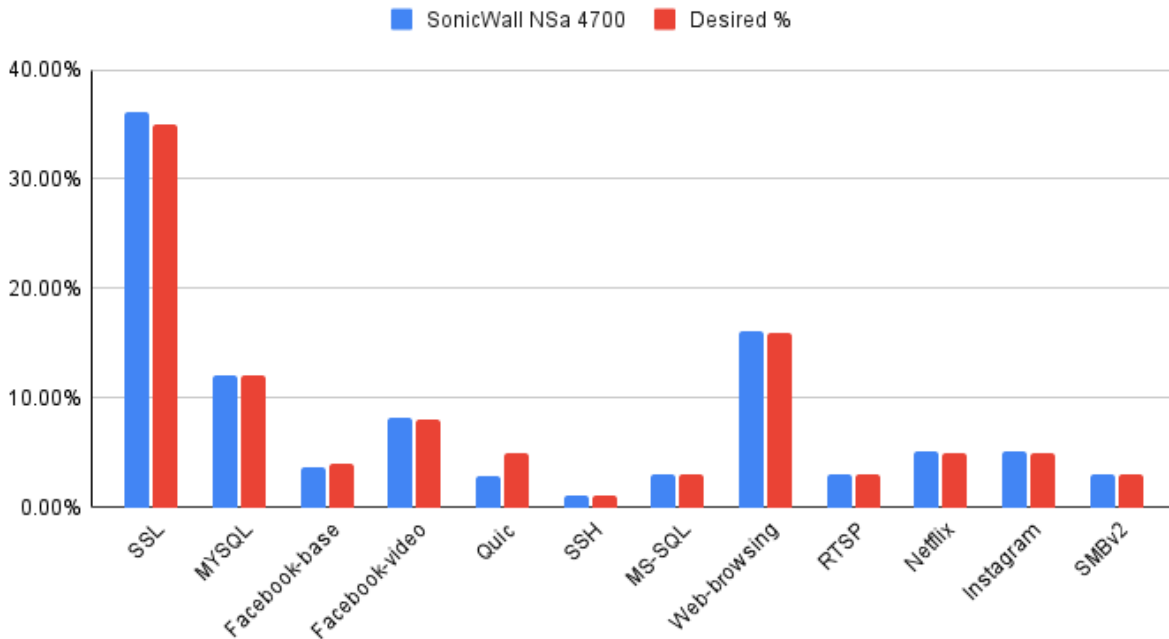


GRAPHS

SonicWall NSa 4700 Healthcare Application Distribution

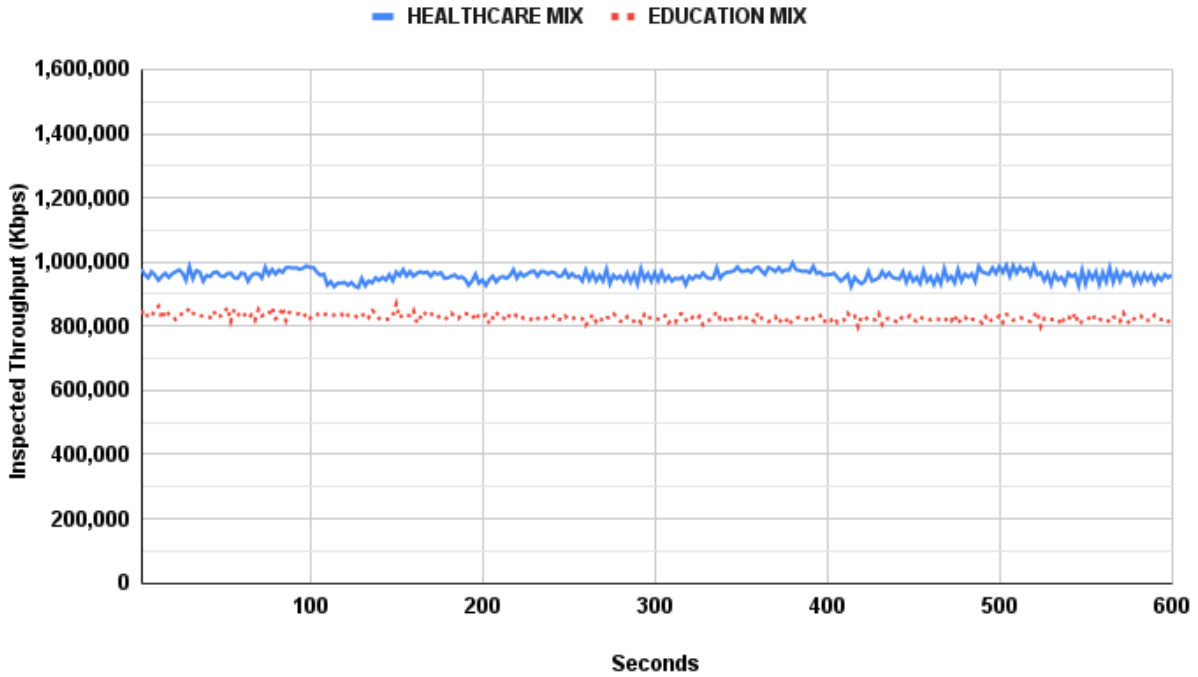


SonicWall NSa 4700 Education Application Distribution

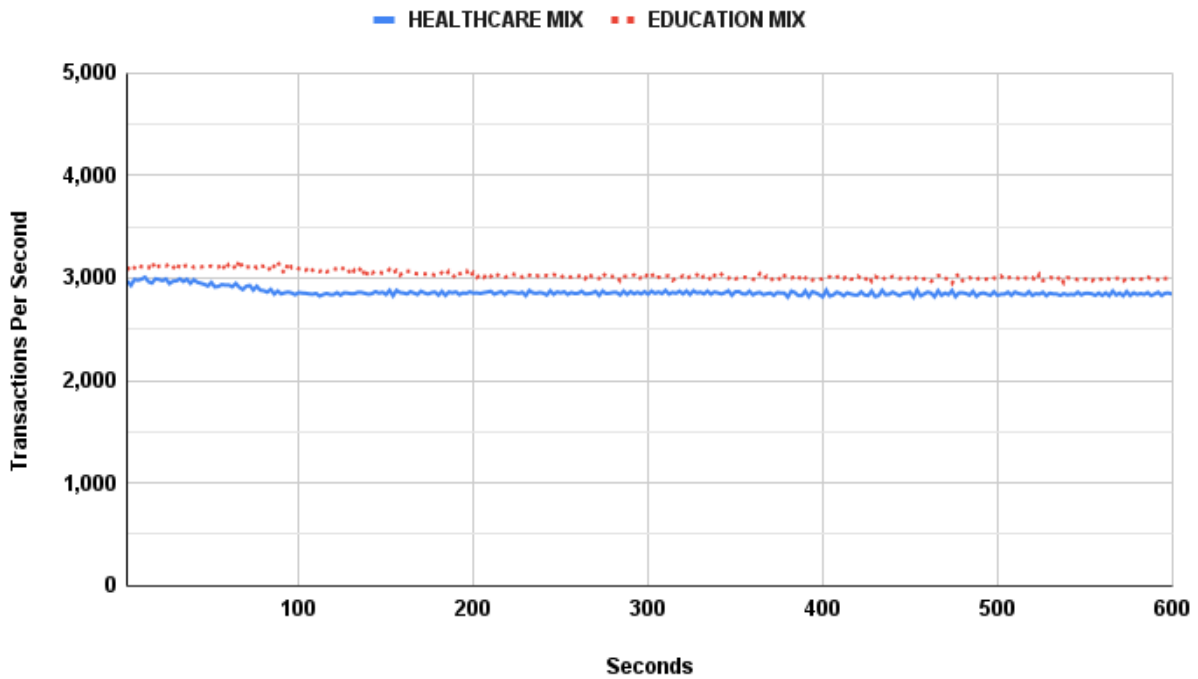


Comparison of desired Inspected Throughput and observed Inspected Throughput for each application within the traffic mixes.

Inspected Throughput Sustained Phase

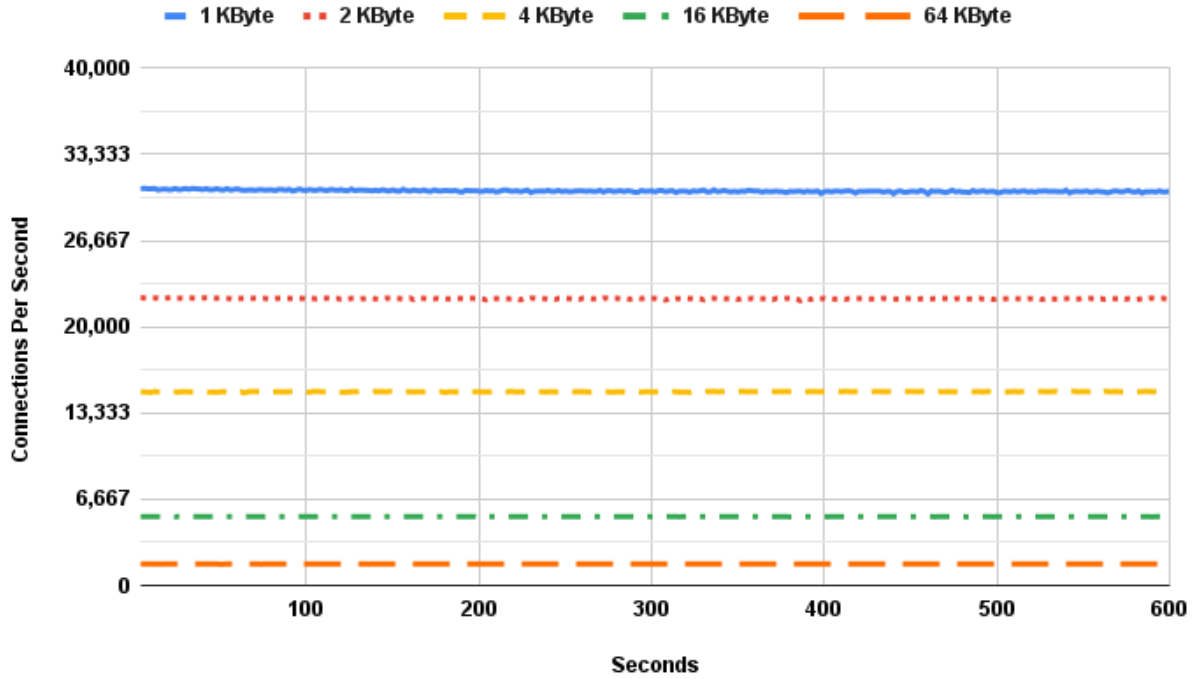


Transactions Per Second Sustained Phase



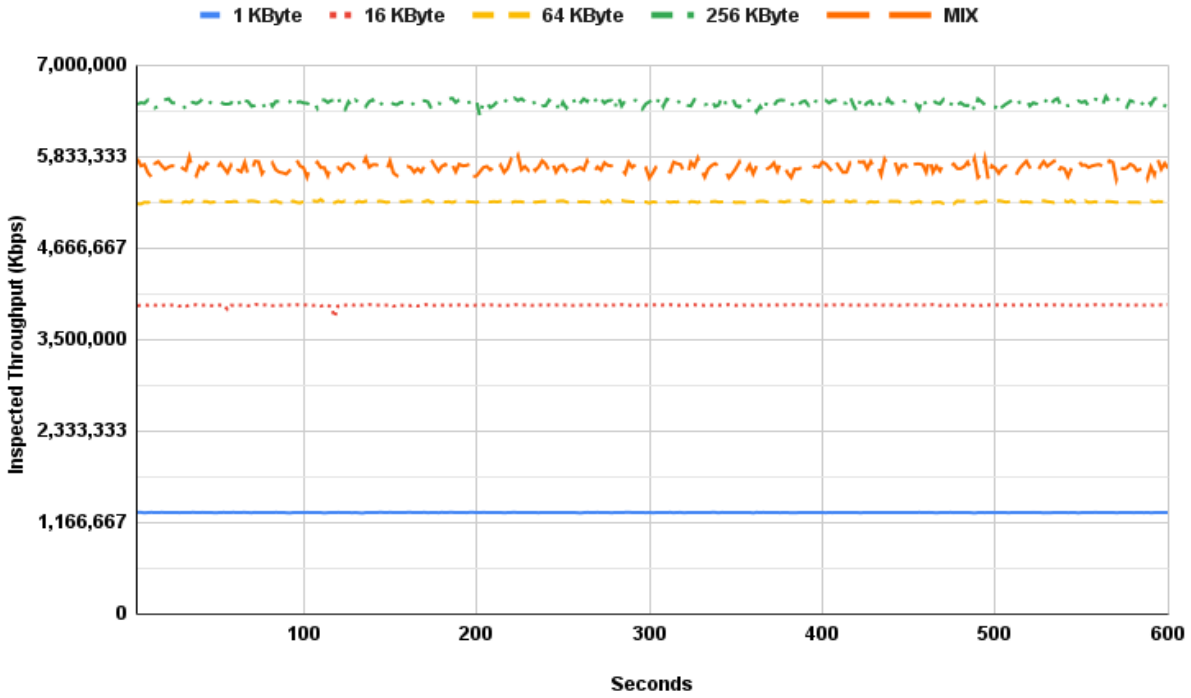
Sustainable inspected throughput of the DUT/SUT for Application Traffic Mixes.

TCP/HTTP Connections Per Second Sustained Phase

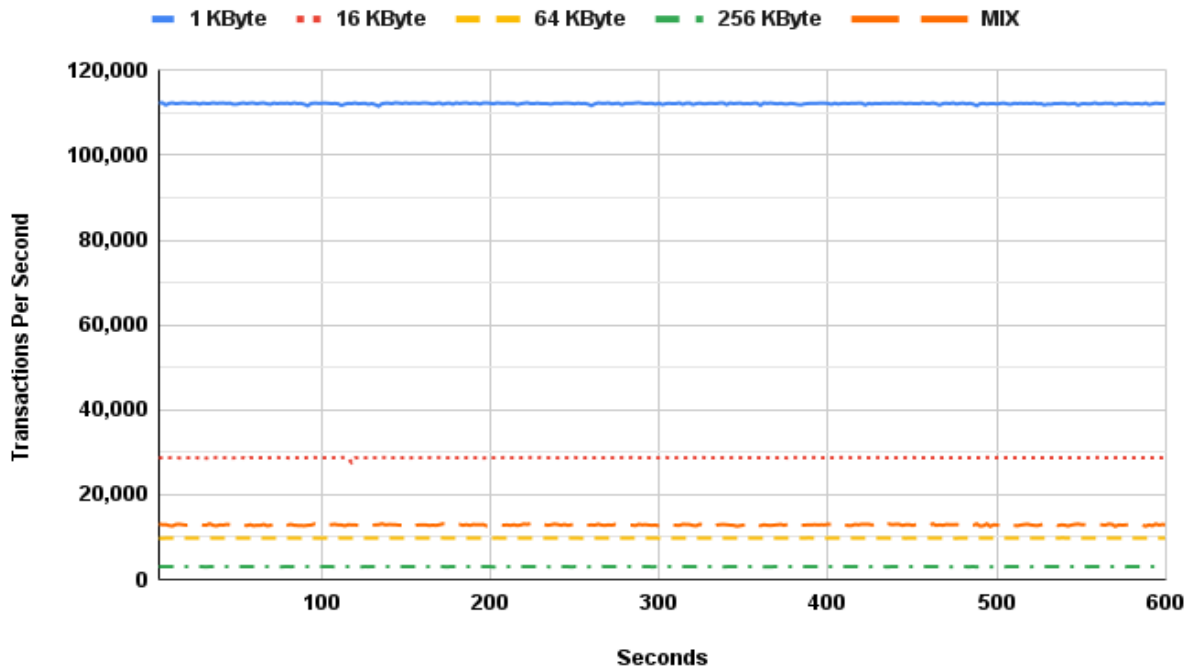


Sustainable TCP/HTTP connection establishment rate supported by the DUT/SUT under different throughput load conditions.

HTTP Inspected Throughput Sustained Phase

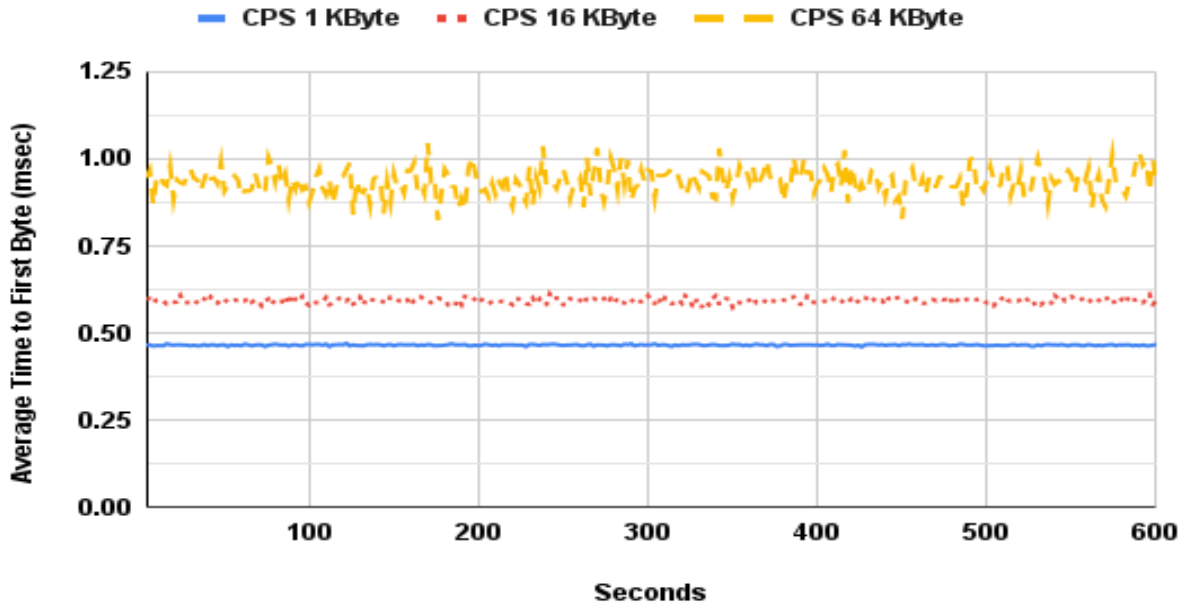


HTTP Transactions Per Second Sustained Phase

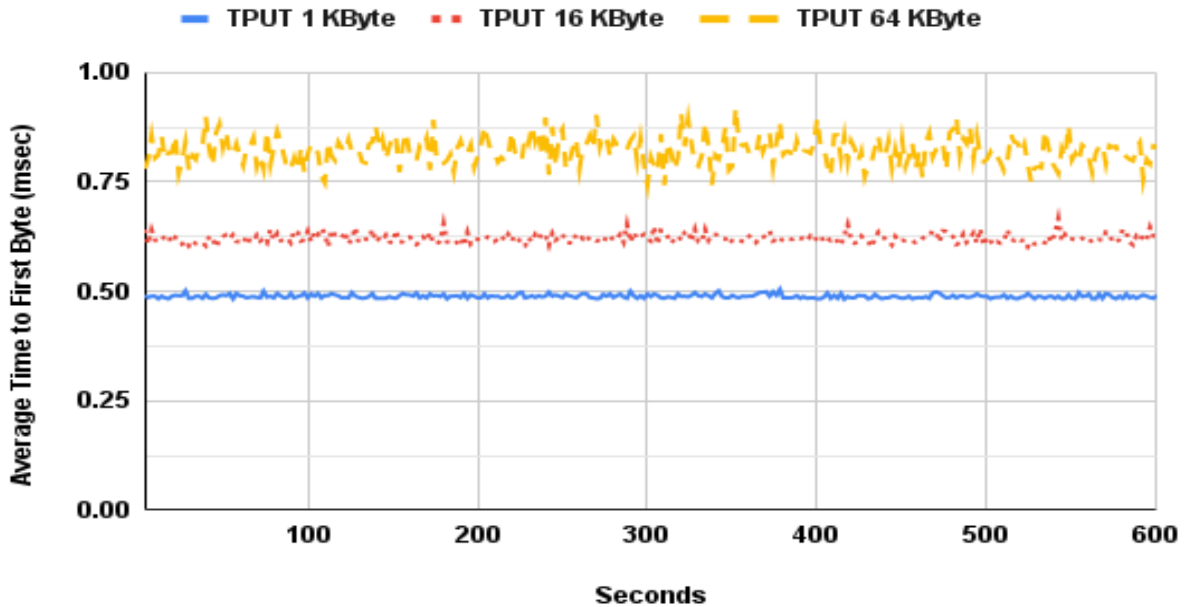


Sustainable inspected throughput of the DUT/SUT for HTTP transactions varying the HTTP response object size.

TCP/HTTP Transaction Latency Connections Per Second Sustained Phase

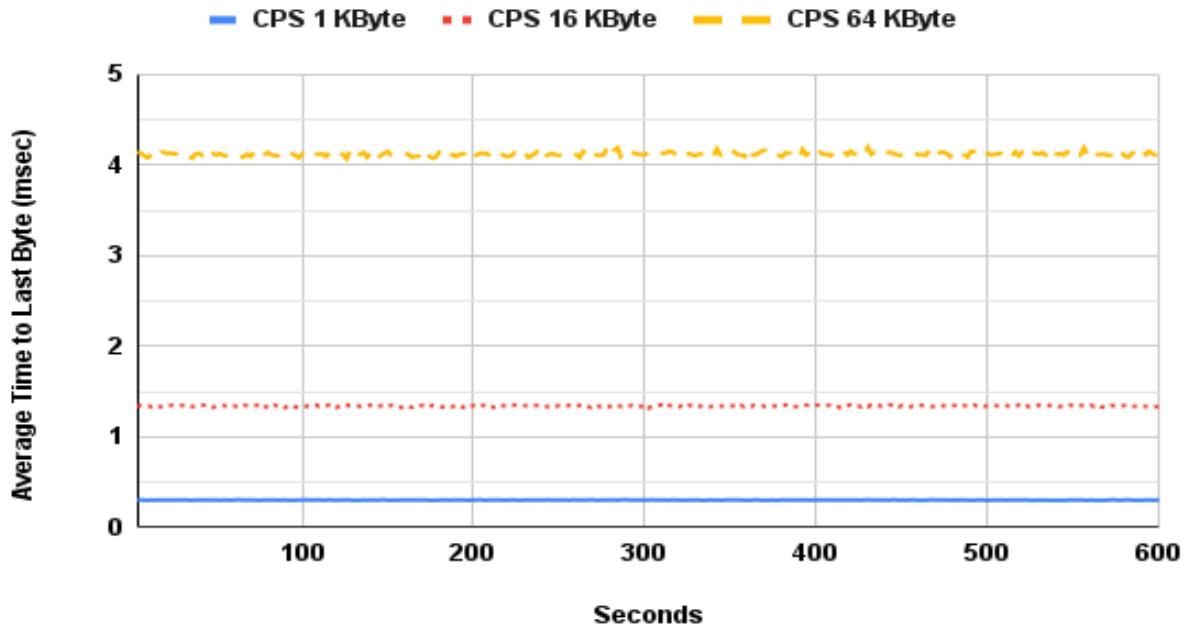


TCP/HTTP Transaction Latency Inspected Throughput Sustained Phase

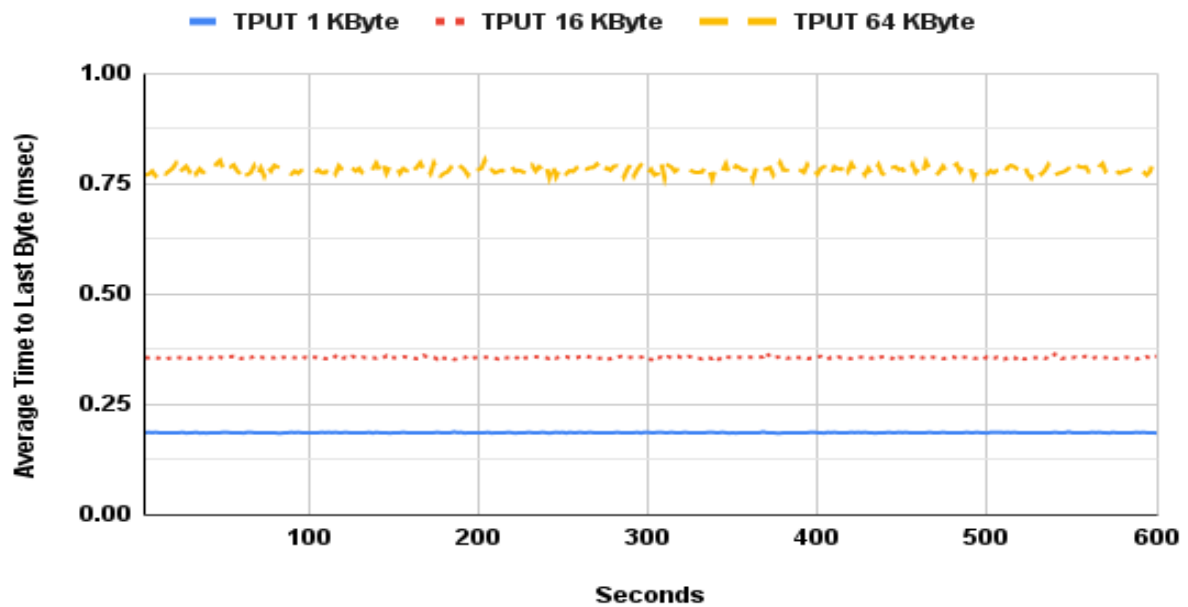


Average HTTP transaction latency time to first byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

TCP/HTTP Transaction Latency Connections Per Second Sustained Phase

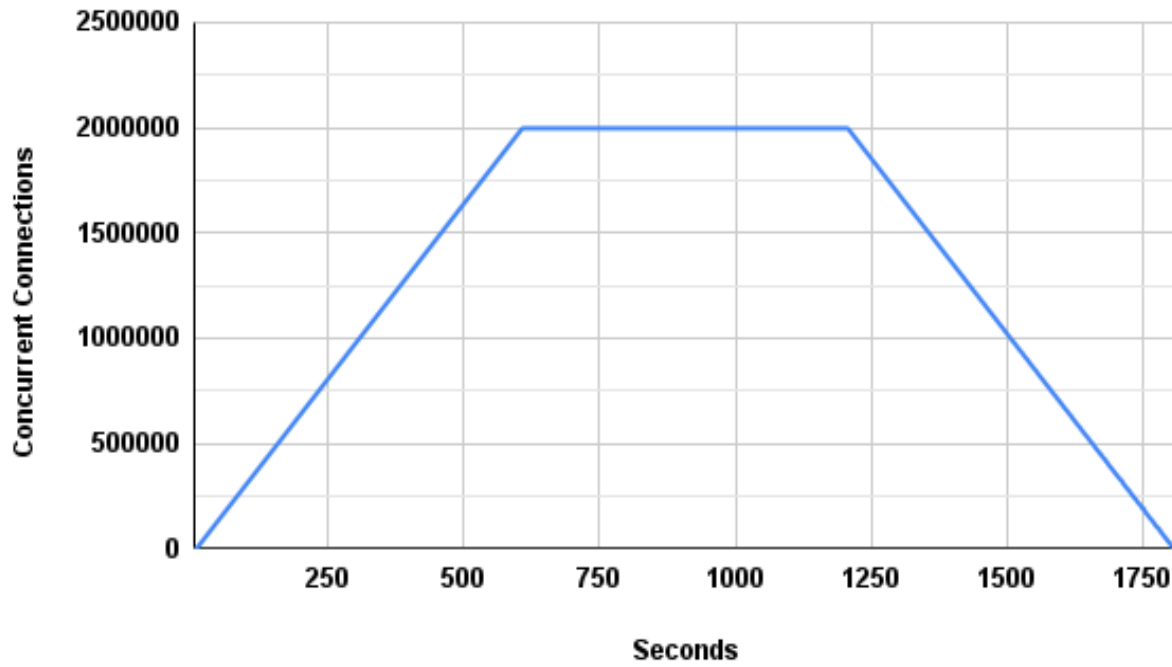


TCP/HTTP Transaction Latency Inspected Throughput Sustained Phase



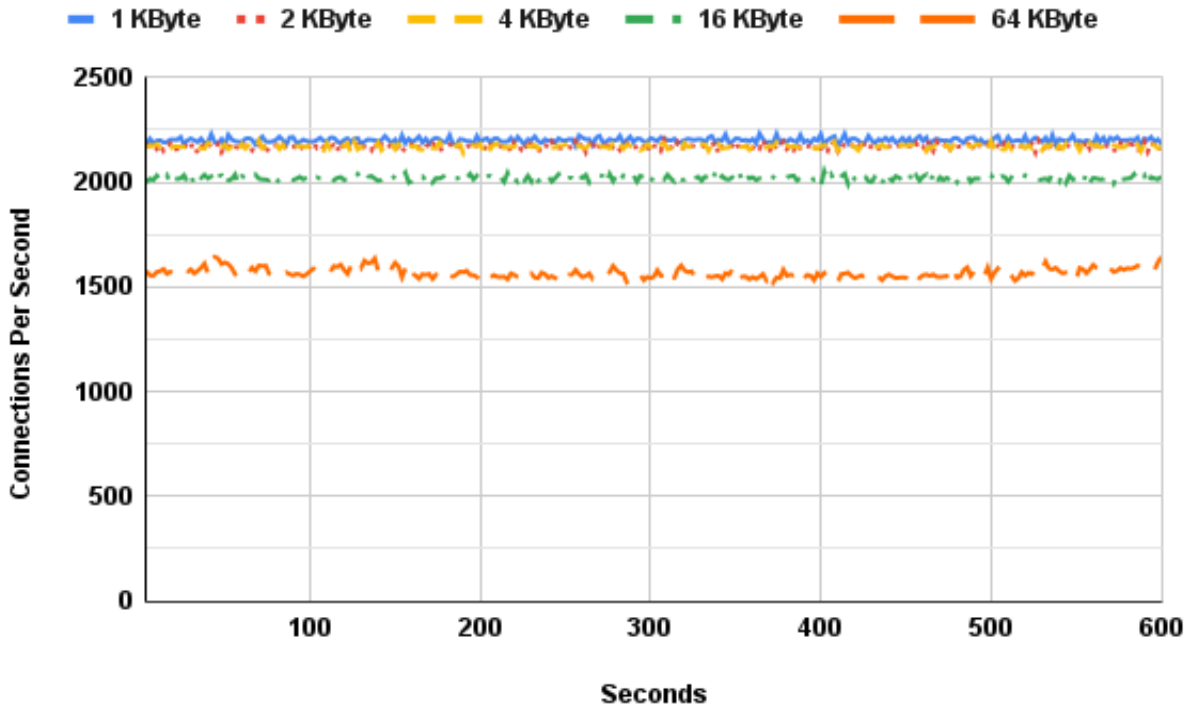
Average HTTP transaction latency time to last byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

Concurrent TCP/HTTP Connection Capacity

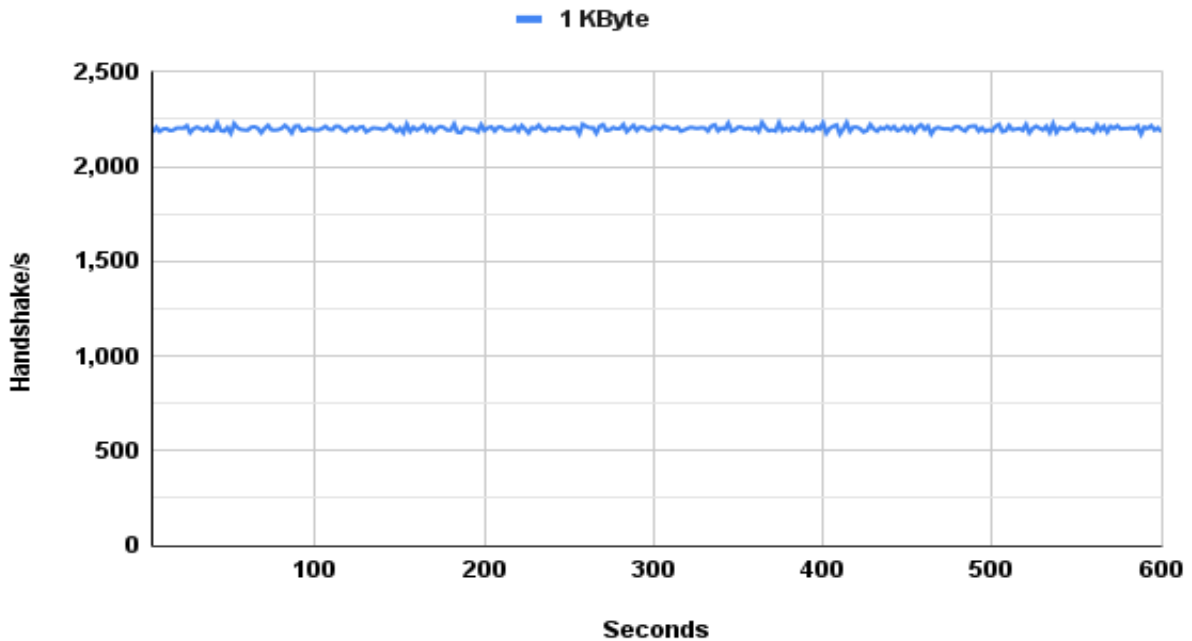


Number of concurrent TCP connections that the DUT/SUT sustains when using HTTP traffic.

TCP/HTTPS Connections Per Second Sustained Phase

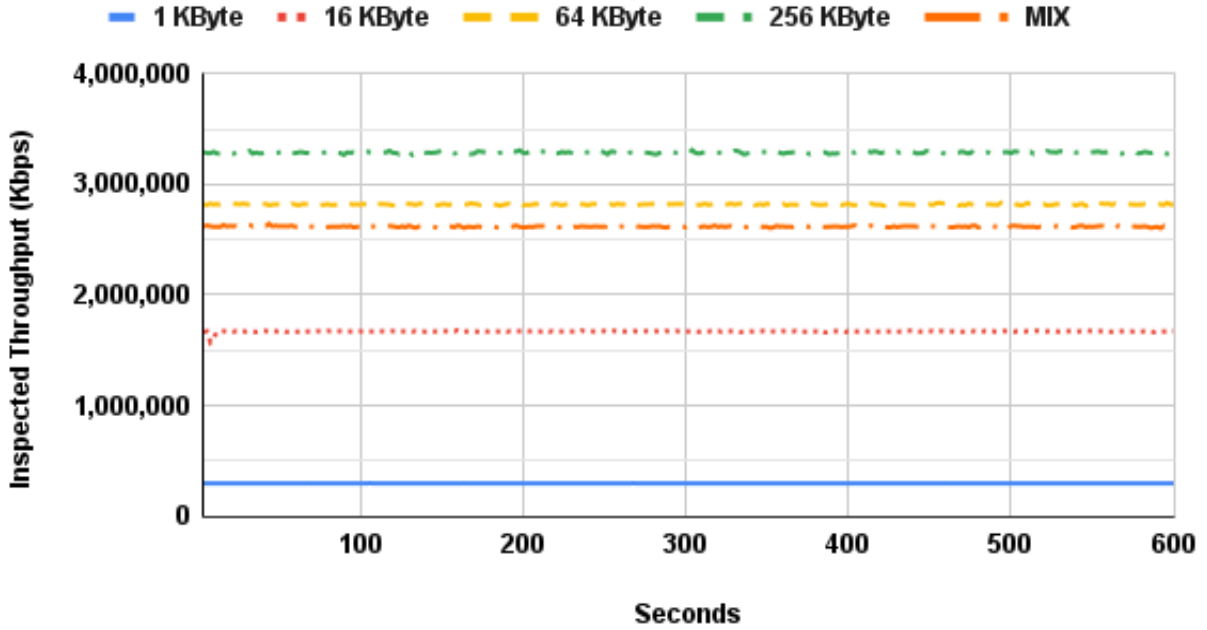


TCP/HTTPS TLS Handshake Rate Sustained Phase

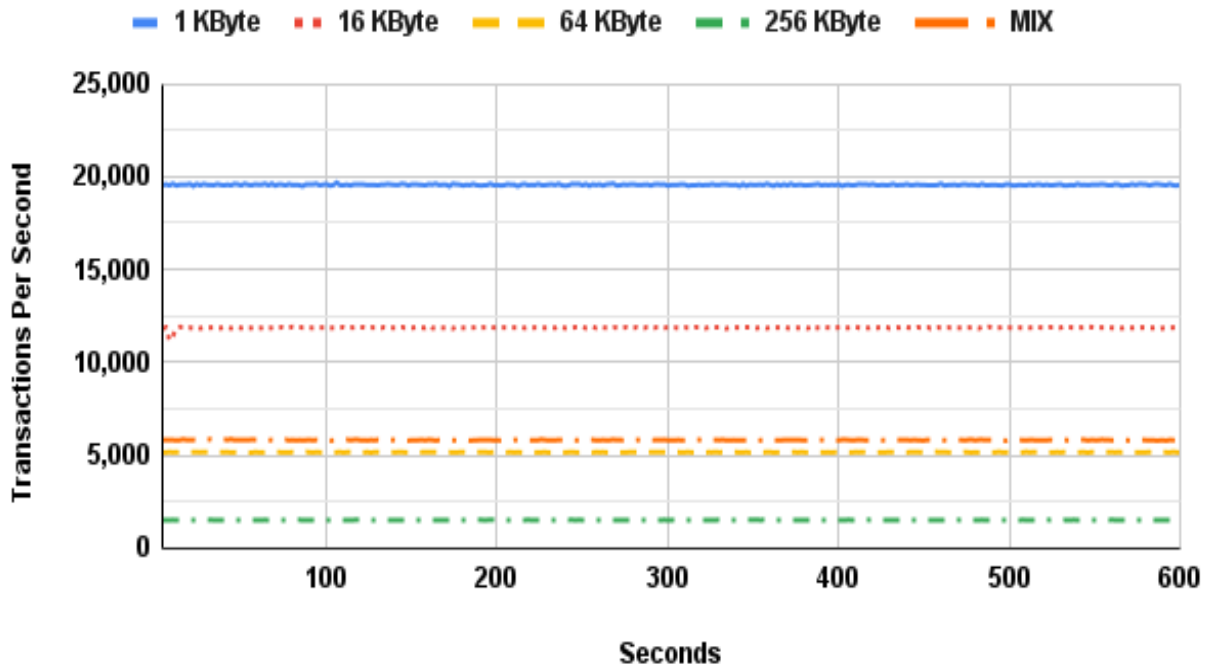


Sustainable SSL/TLS session establishment rate supported by the DUT/SUT under different throughput load conditions.

HTTPS Inspected Throughput Sustained Phase

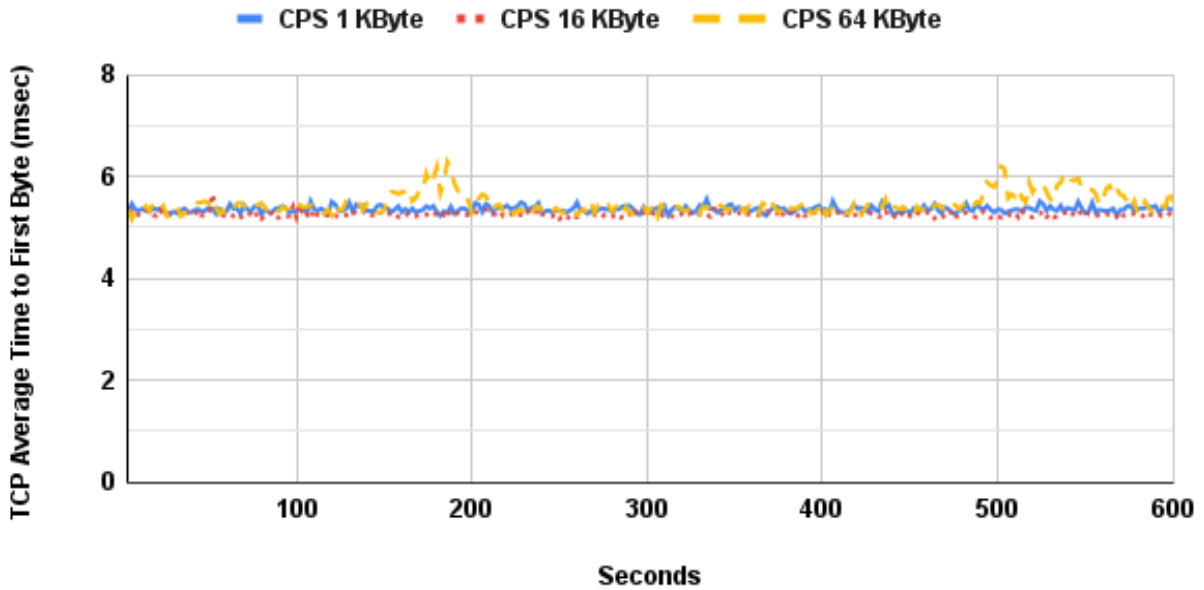


HTTPS Transactions Per Second Sustained Phase

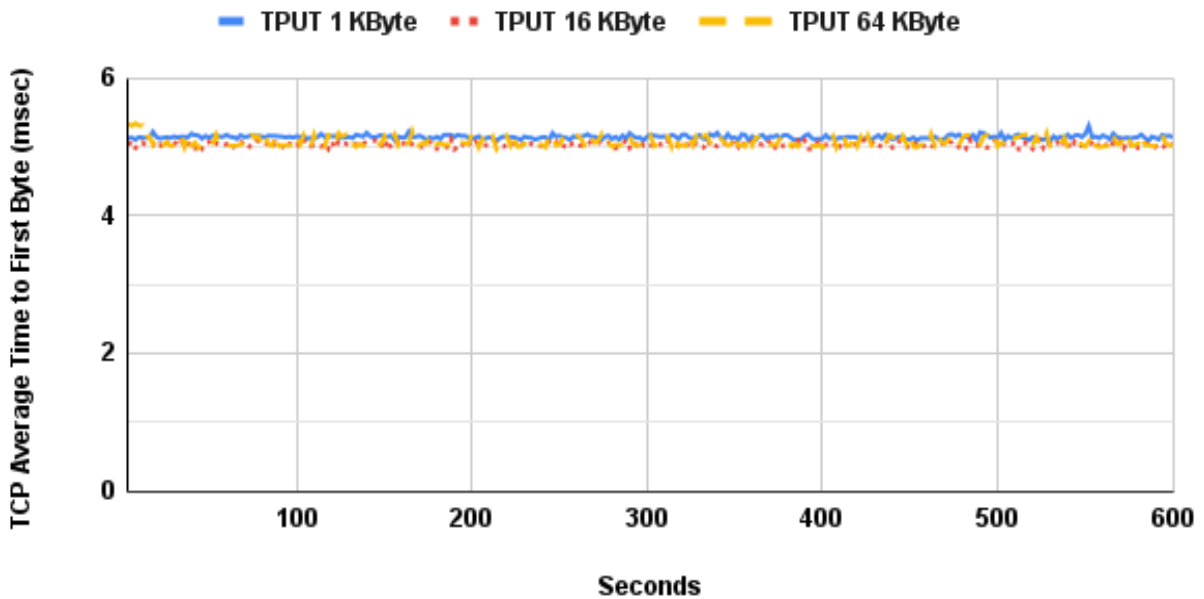


Sustainable inspected throughput of the DUT/SUT for HTTPS transactions varying the HTTPS response object size.

TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase

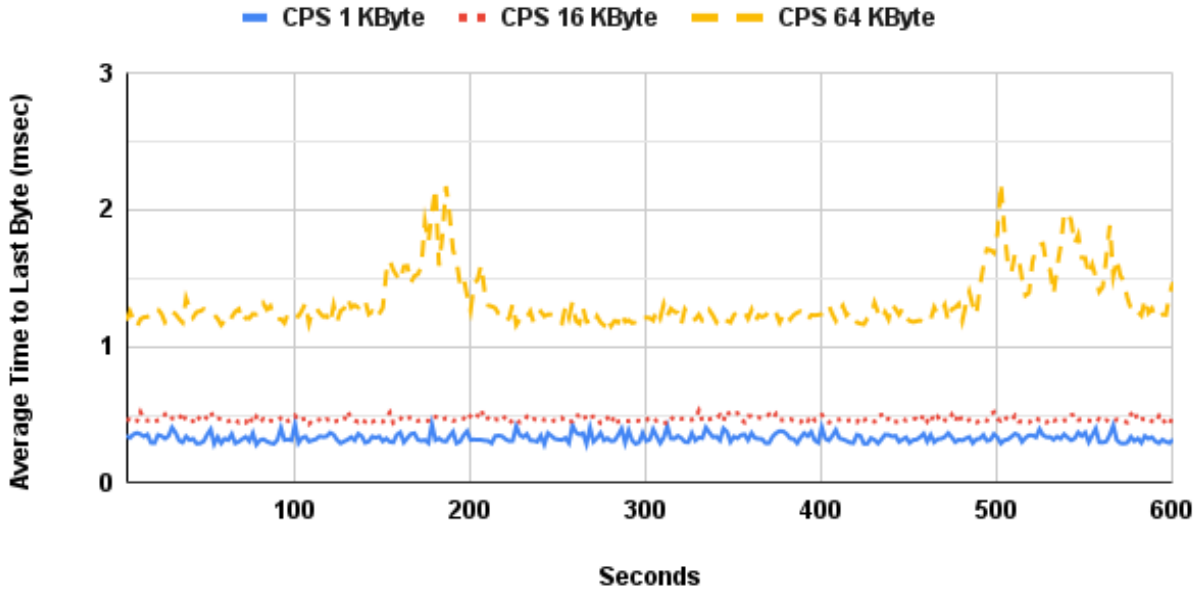


TCP/HTTPS Transaction Latency Inspected Throughput Sustained Phase

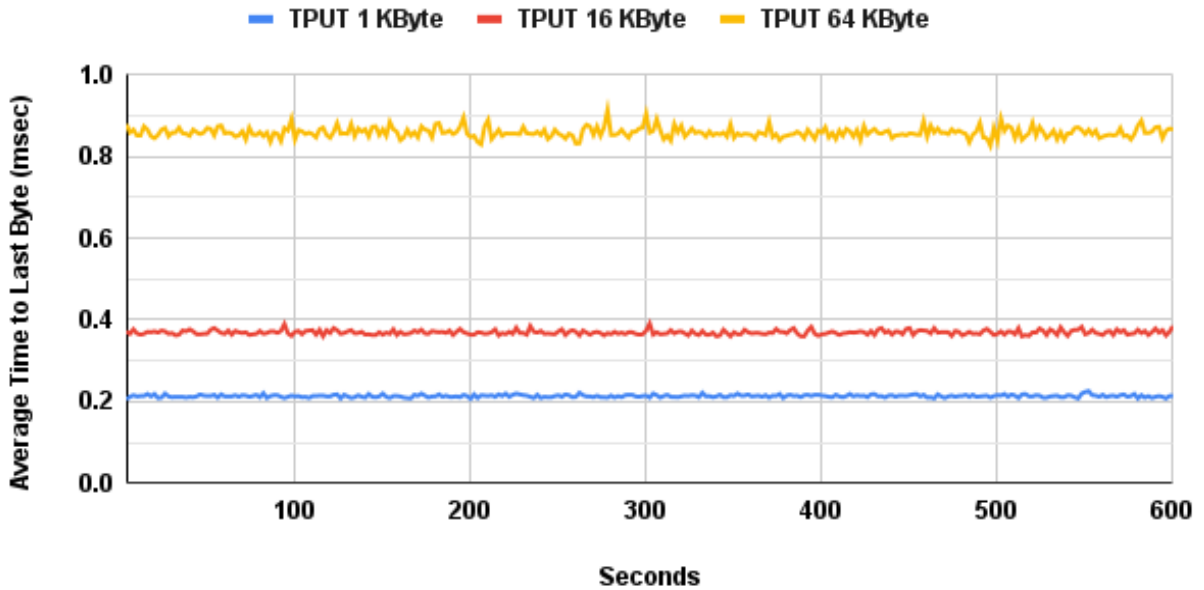


Average HTTPS transaction latency time to first byte under different HTTPS response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase

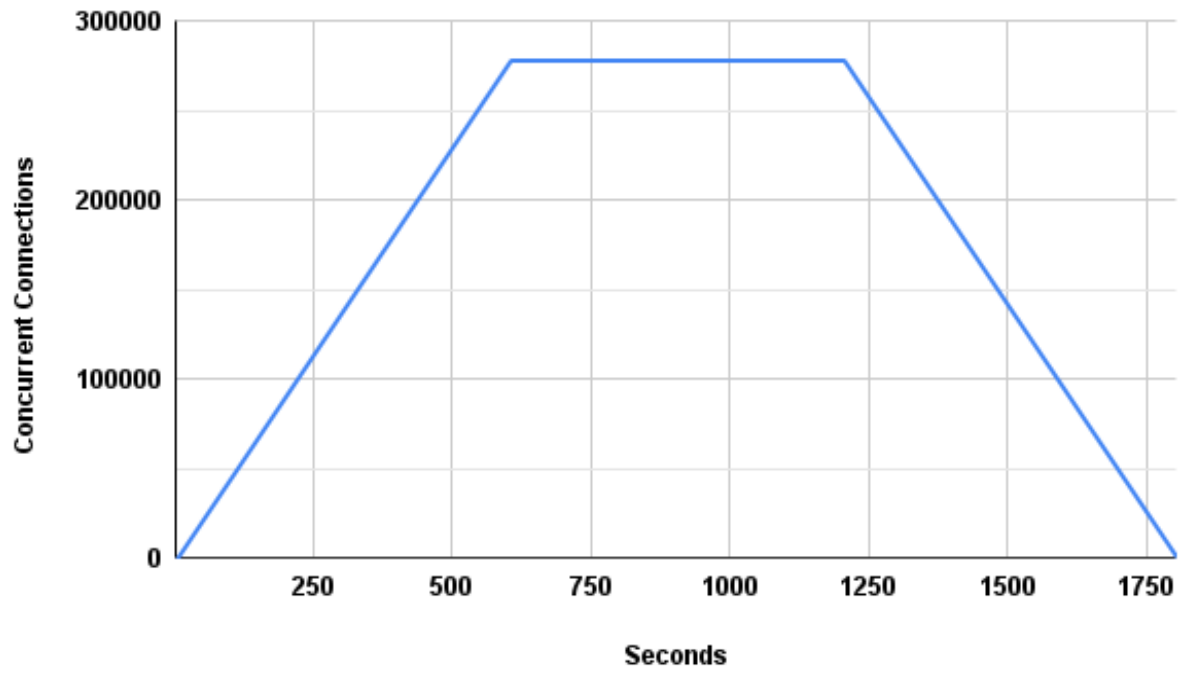


TCP/HTTPS Transaction Latency Inspected Throughput Sustained Phase



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	1,380	1,380	0
Private CVE	180	180	0
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 Gbps (Kbps)	0.91 (912,733)				0.76 (763,233)			
	TPS	3,084				2,738			
	CVE	Unique CVEs	Scenarios total	Blocked	Not Blocked	Unique CVEs	Scenarios total	Blocked	Not Blocked
		50	2,060	2,060	0	50	2,020	2,020	0

