University of New Hampshire
InterOperability Laboratory

NetSecOPEN

TEST REPORT

August 2024

www.iol.unh.edu

RYAN LILES
CISCO SYSTEMS
RYLILES@CISCO.COM

DEVICE AND TEST PLAN INFORMATION	
Device Under Test (DUT)	Cisco Secure Firewall 3105
Test Specification/Suite	Benchmarking Methodology for Network Security Device Performance RFC 9411
UNH-IOL Test Result ID	38476

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: 2024.08.20 12:22:11 -04'00'

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	08/19/2024	Chris Brown	Initial version

DEVICE INFORMATION

COMPONENT	DESCRIPTION
Device Name	Cisco Secure Firewall 3105
UNH-IOL Device Identification Number	FW-CSCO-0000030780
Device Model	3105
Software Version	7.4.1.1
Operating System Version	FX-OS 2.14.1
Vulnerability Database (VDB)	388
Snort Rule Update Version	2024-08-02-001-vrt
Lightweight Security Package (LSP)	lsp-rel-20240802-1505
Controller Model	Secure Firewall Management Center for VMware
Software Version	7.4.1.1
Operating System Version	FX-OS 2.14.1
Interfaces Tested	Ethernet1/9, ethernet1/10, ethernet1/11, ethernet1/12
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	2
IP Layer	Allow	2

TEST TOOL AND ENVIRONMENT INFORMATION

COMPONENT	DESCRIPTION	
Performance Test Equipment Vendor	Spirent	
Performance Hardware Name	SPT-C100-S3	
Performance Hardware Firmware	5.47.3813	
Performance Hardware Interface Type	10G	
Performance Application Software Name	Cyberflood	
Performance Application Software Version	24.3.1012	
Test Equipment Vendor	Ixia	
Security Effectiveness Hardware Name	PerfectStorm One	
Security Effectiveness Hardware Firmware	10.00.1000.14	
Security Effectiveness Hardware Interface Type	10G	
Security Effectiveness Application Software Name	BreakingPoint	
Security Effectiveness Application Software Version	10.00.1.74	
Security Effectiveness Application and Threat Intelligence (ATI) Strikepack Version	2024-13	
Client IP Subnet 1	10.10.0.0/23	
Server IP Subnet 1	10.11.0.0/23	
Client IP Subnet 2	10.12.0.0/23	
Server IP Subnet 2	10.13.0.0/23	
Traffic Distribution Ratio	**IPv4**	**IPv6**
	100%	0%
Cipher Suite	ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048	

TESTBED SETUP

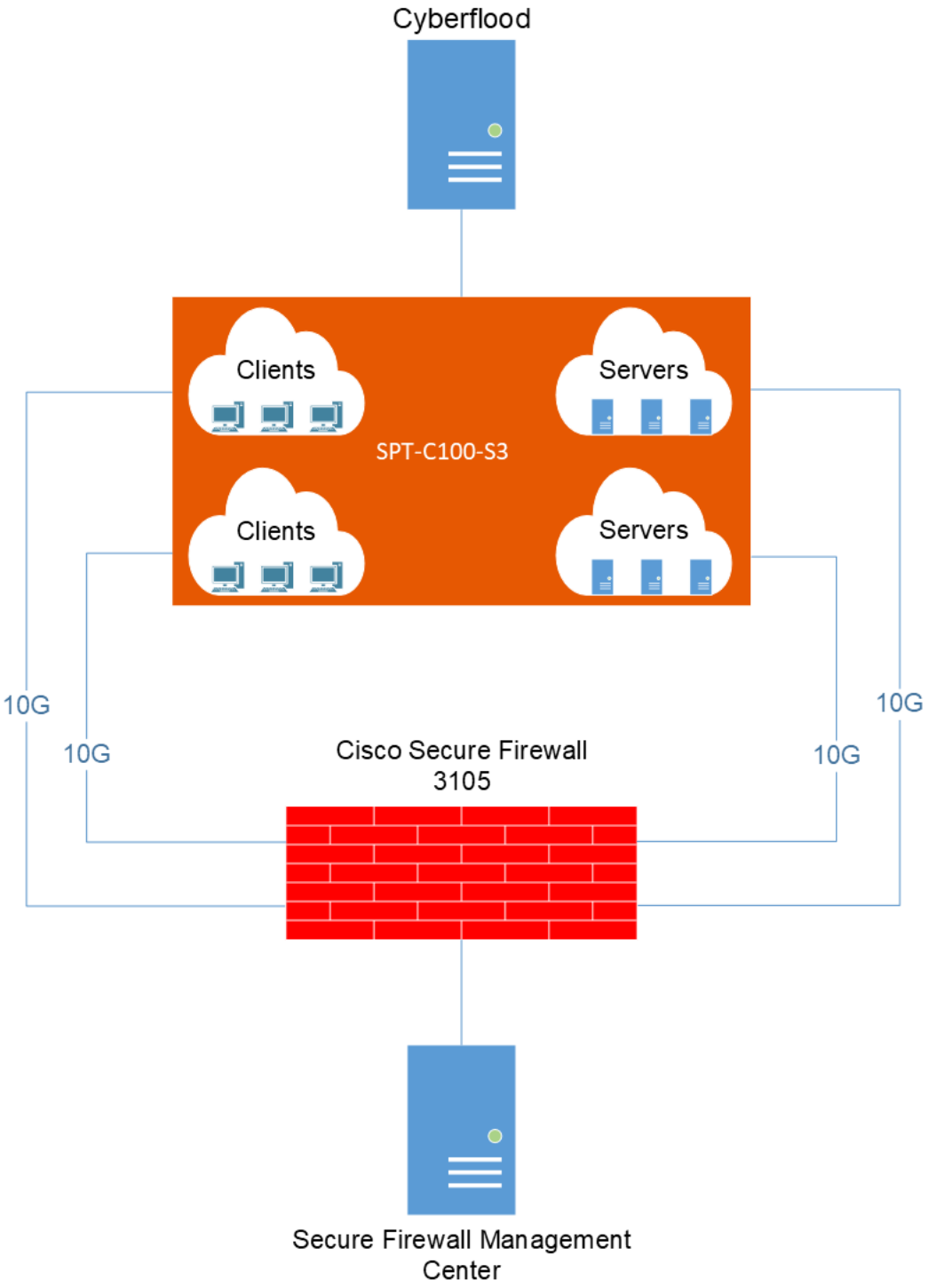


Figure 1: Topology with Performance Test Equipment Vendor

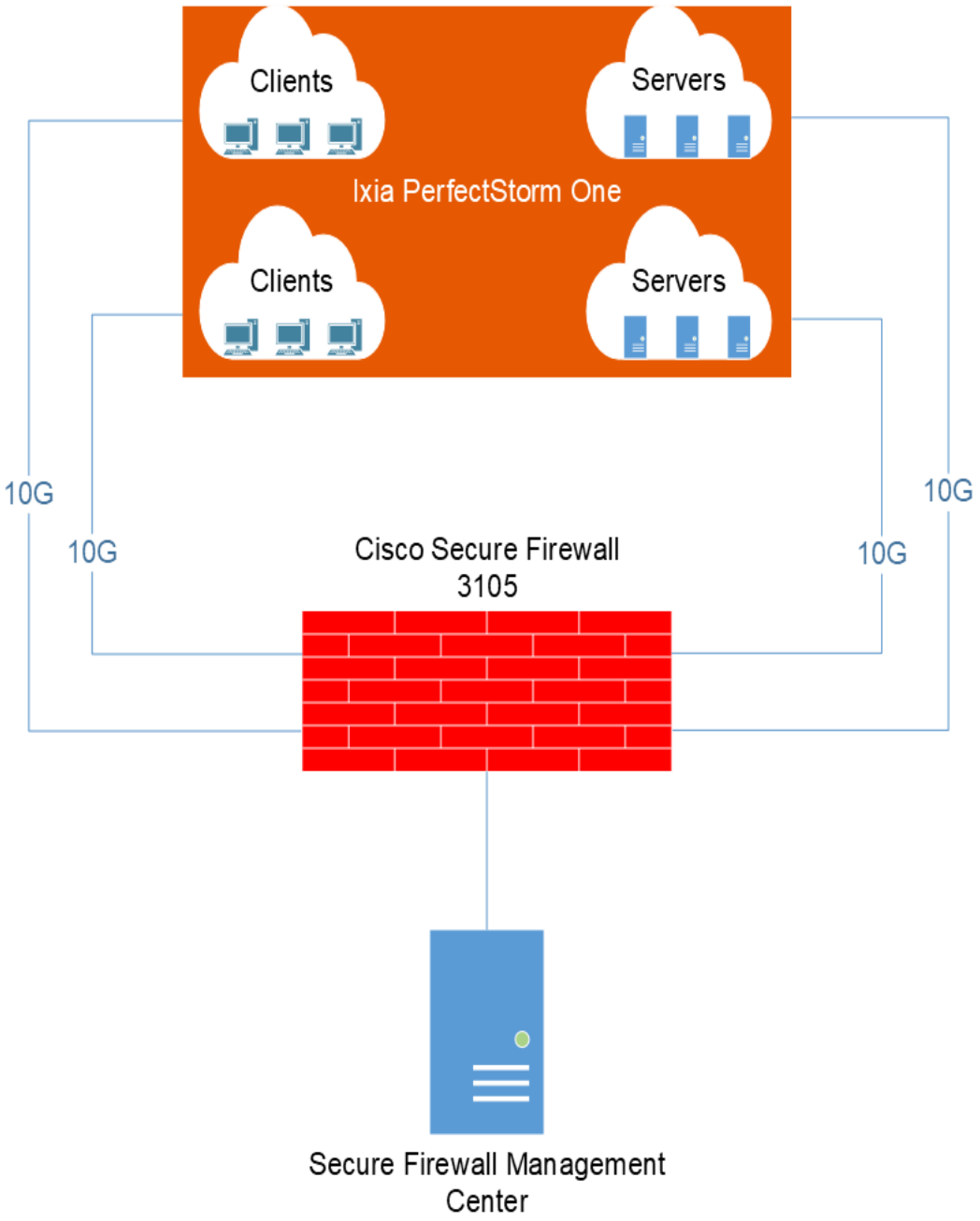


Figure 2: Topology with Security Effectiveness Test Equipment Vendor

SECURITY EFFECTIVENESS SUMMARY

SCENARIO	TOTAL	BLOCKED	ALLOWED	BLOCK RATE
Public CVE	1,380	1,354	26	98.11%
Private CVE	180	173	7	96.11%
Malware	3,809	3,773	35	99.05%
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)	3.44 (3,437,000)	3.02 (3,018,000)
TPS	14,292	16,801
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)	3.59 (3,589,000)	3.16 (3,164,000)
	TPS	15,030	17,691

SECTION 7.2

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTP Connections Per Second	CPS	42,366	40,245	38,007	28,183	13,889

SECTION 7.3

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTP Inspected Throughput	TPUT Gbps (Kbps)	0.92 (922,303)	5.84 (5,835,252)	10.16 (10,161,288)	11.25 (11,253,677)	9.48 (9,484,208)
	TPS	80,018	42,548	18,838	5,241	21,407

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)	1.630	1.243	1.309	1.532	1.130	1.514
	TTFB Minimum (msec)	1.623	1.234	1.292	1.510	1.108	1.469
	TTFB Maximum (msec)	1.637	1.252	1.329	1.560	1.183	1.593
	TTLB Average (msec)	0.861	1.224	2.706	0.751	0.728	1.634
	TTLB Minimum (msec)	0.855	1.216	2.686	0.744	0.721	1.606
	TTLB Maximum (msec)	0.869	1.233	2.729	0.758	0.736	1.663

SECTION 7.5

TEST CASE	KPI	1K
Concurrent TCP/HTTP Connection Capacity	CC	1,999,872

SECTION 7.6

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTPS Connections Per Second	CPS	6,922	6,796	6,733	6,300	4,927
	HR	1K				
		6,922				

SECTION 7.7

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTPS Inspected Throughput	TPUT Gbps (Kbps)	0.55 (549,418)	3.55 (3,554,412)	4.54 (4,540,805)	4.55 (4,545,007)	4.17 (4,166,422)
	TPS	38,352	24,985	8,224	2,076	9,175

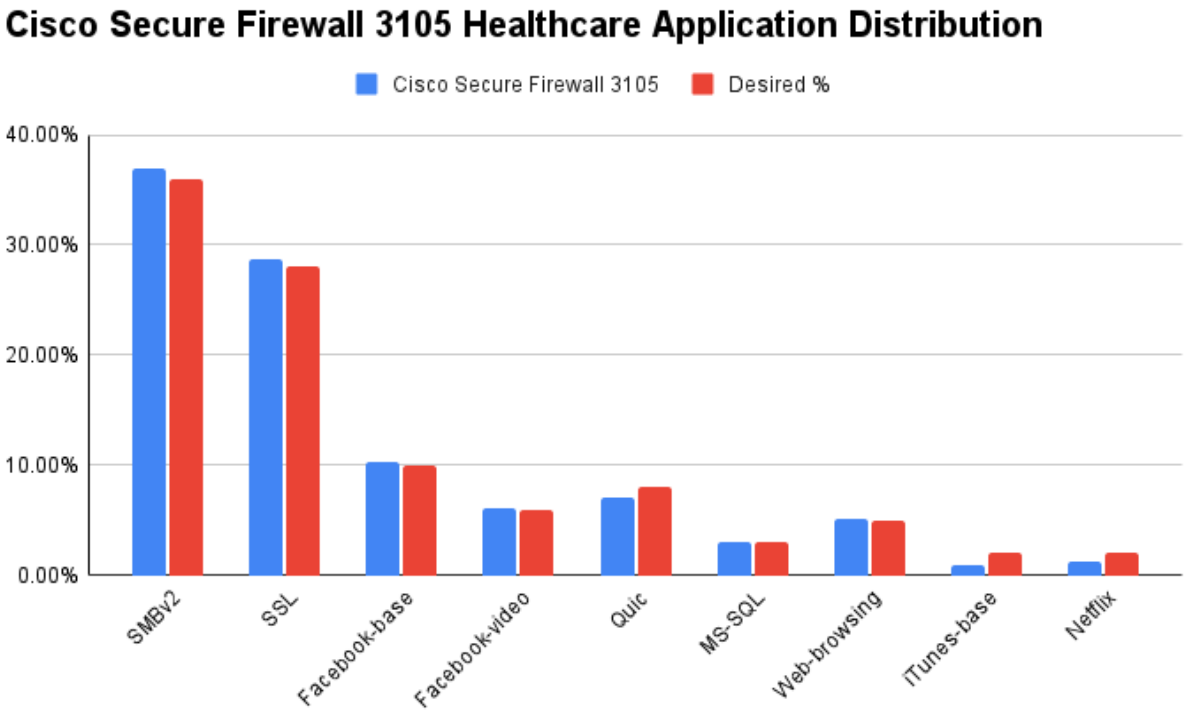
SECTION 7.8

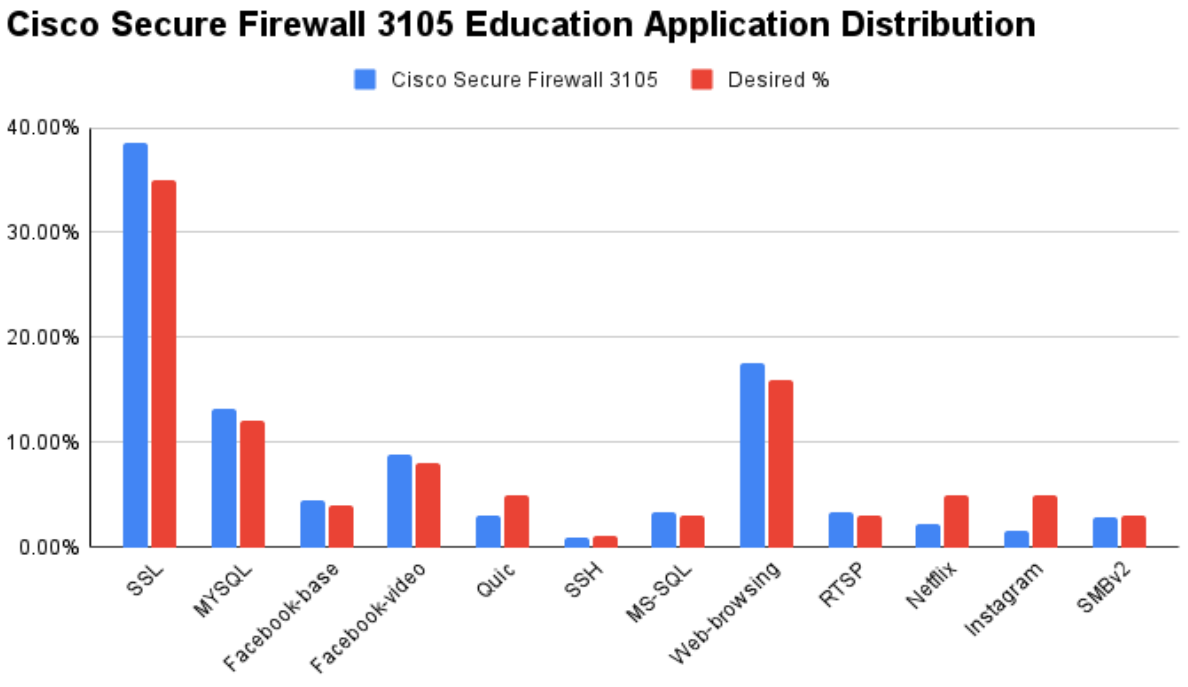
TEST CASE	KPI	CPS 1K	CPS 16K	CPS 64K	TPUT 1K	TPUT 16K	TPUT 64K
TCP/HTTPS Transaction Latency	TTFB Average (msec)	3.110	3.011	3.015	3.020	2.782	3.010
	TTFB Minimum (msec)	3.078	2.969	2.975	2.980	2.744	2.959
	TTFB Maximum (msec)	3.144	3.058	3.057	3.089	2.844	3.400
	TTLB Average (msec)	1.122	1.765	2.581	1.014	1.648	2.287
	TTLB Minimum (msec)	1.106	1.741	2.544	1.006	1.635	2.258
	TTLB Maximum (msec)	1.146	1.791	2.640	1.025	1.663	2.319

SECTION 7.9

TEST CASE	KPI	1K
Concurrent TCP/HTTPS Connection Capacity	CC	149,040

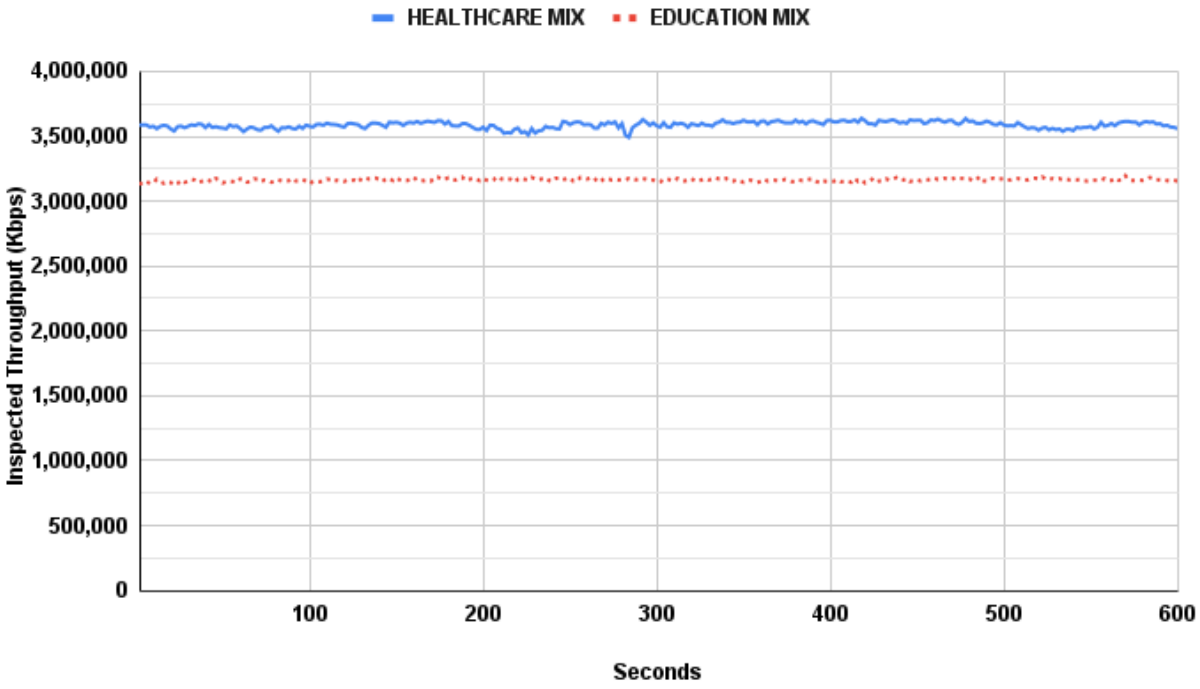
GRAPHS



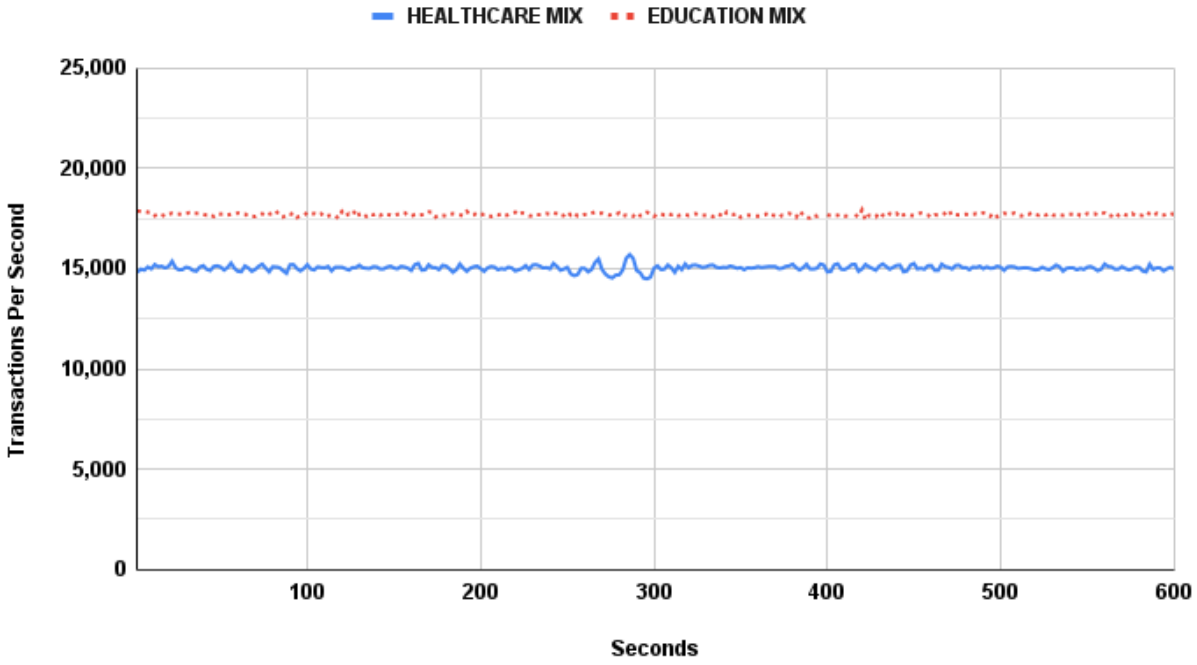


Comparison of desired Inspected Throughput and observed Inspected Throughput for each application within the traffic mixes.

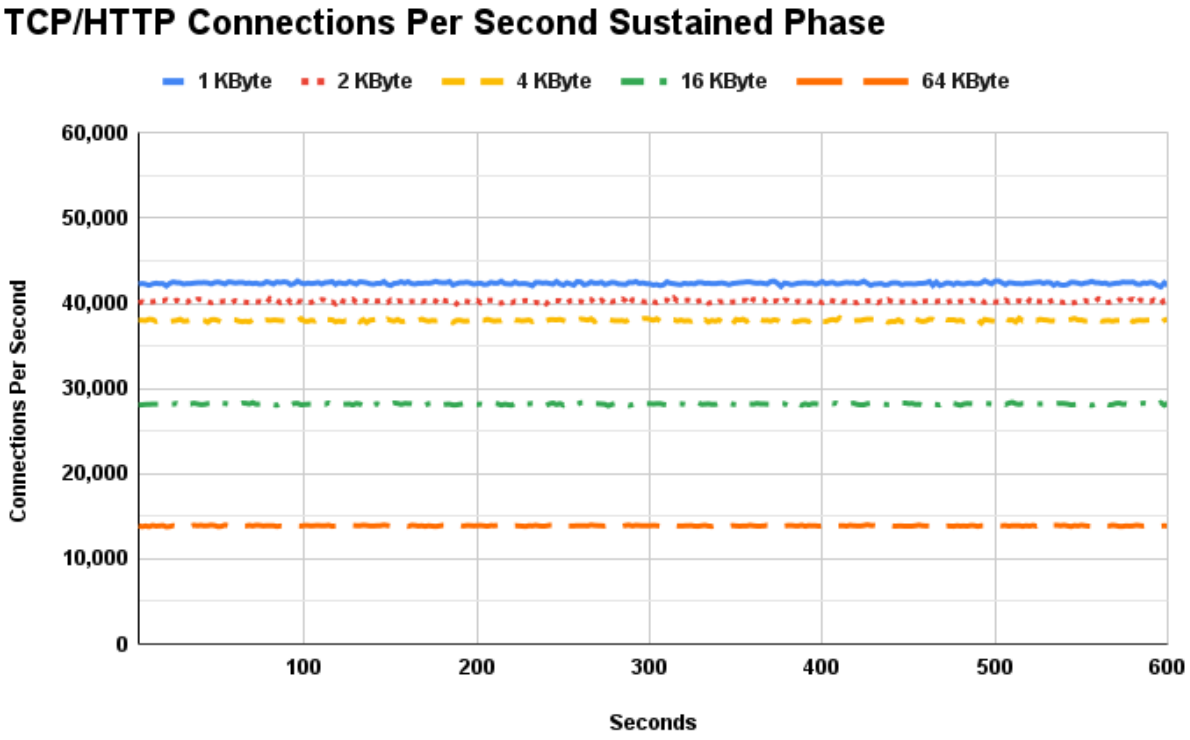
Inspected Throughput Sustained Phase



Transactions Per Second Sustained Phase

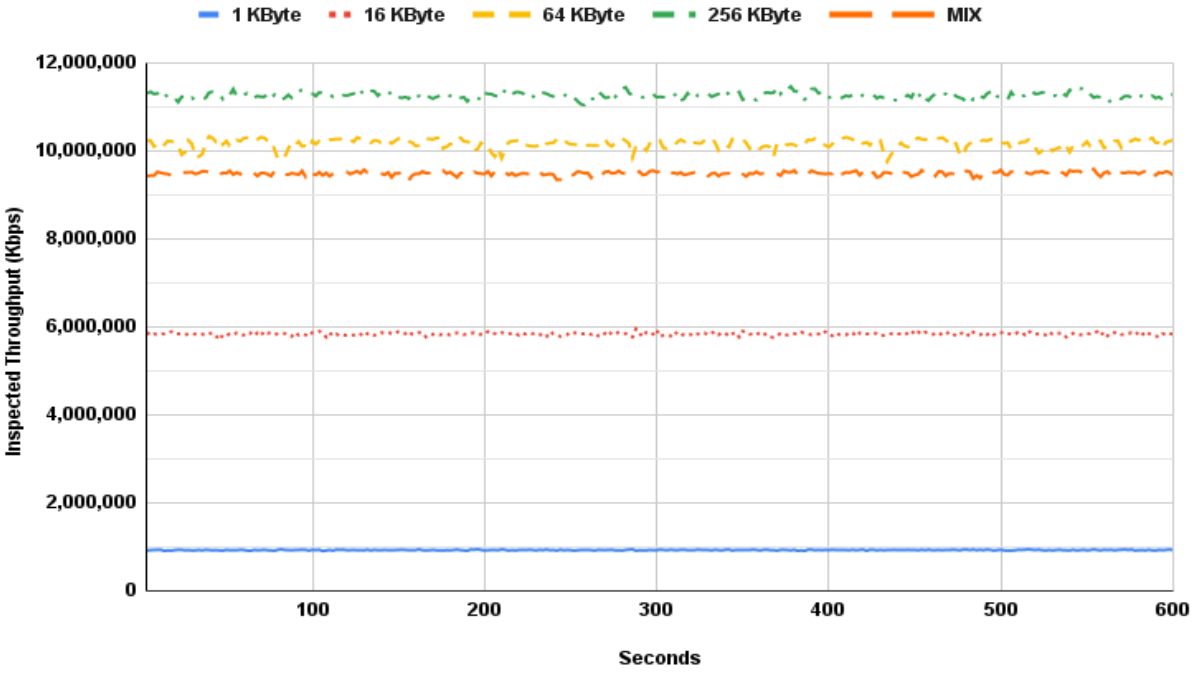


Sustainable inspected throughput of the DUT/SUT for Application Traffic Mixes.

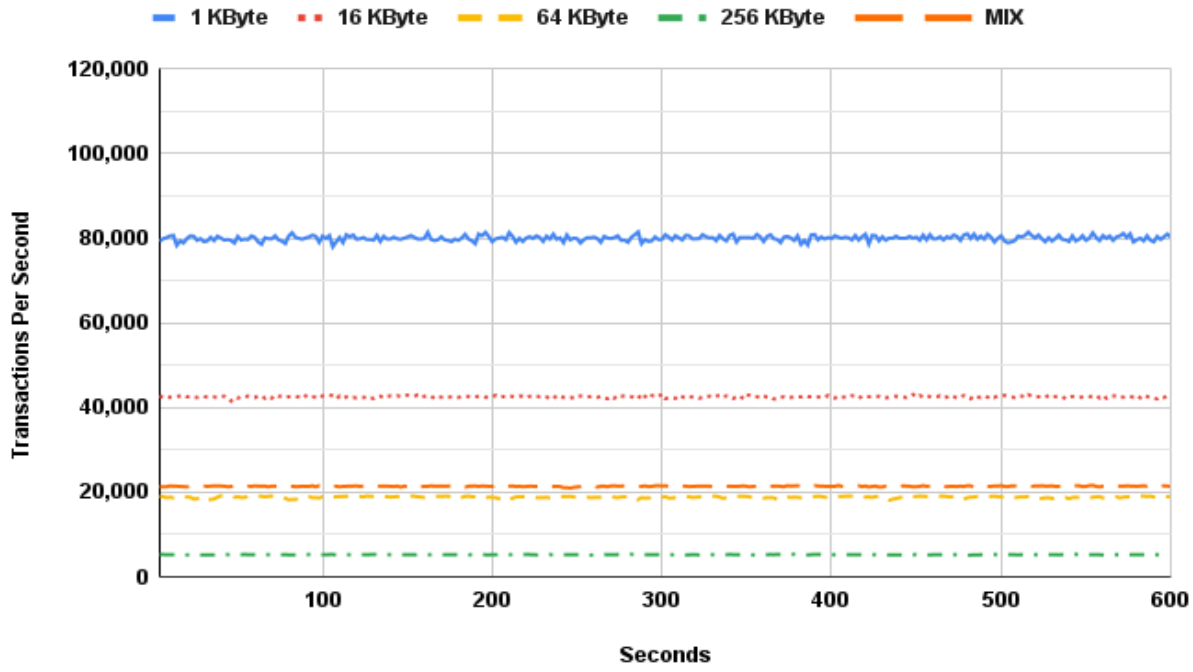


Sustainable TCP/HTTP connection establishment rate supported by the DUT/SUT under different throughput load conditions.

HTTP Inspected Throughput Sustained Phase

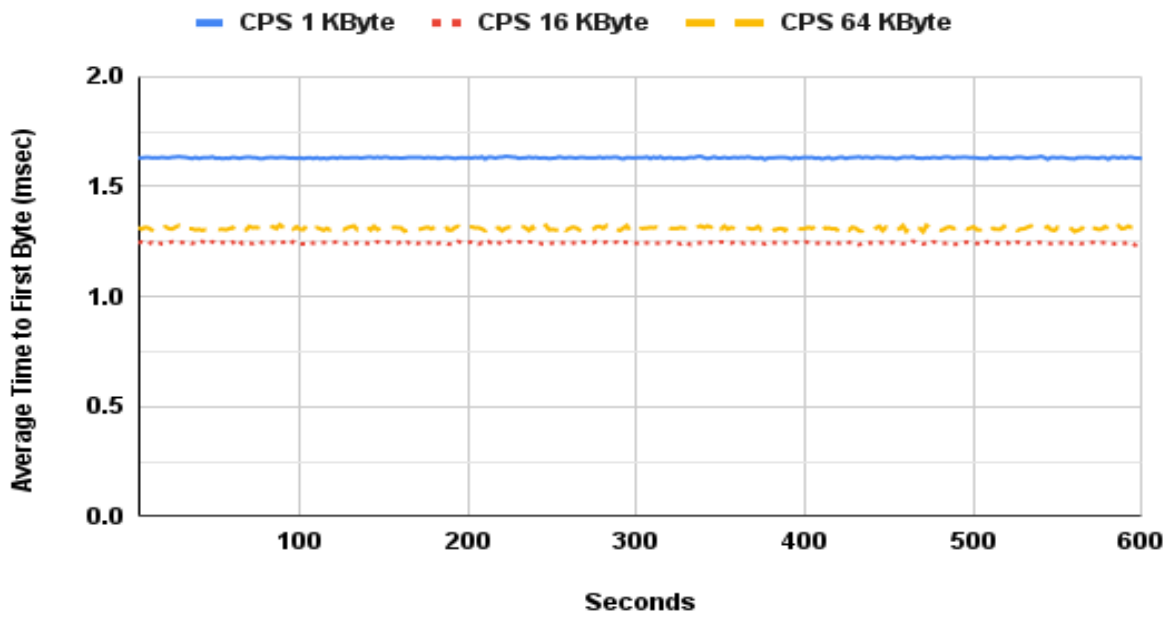


HTTP Transactions Per Second Sustained Phase

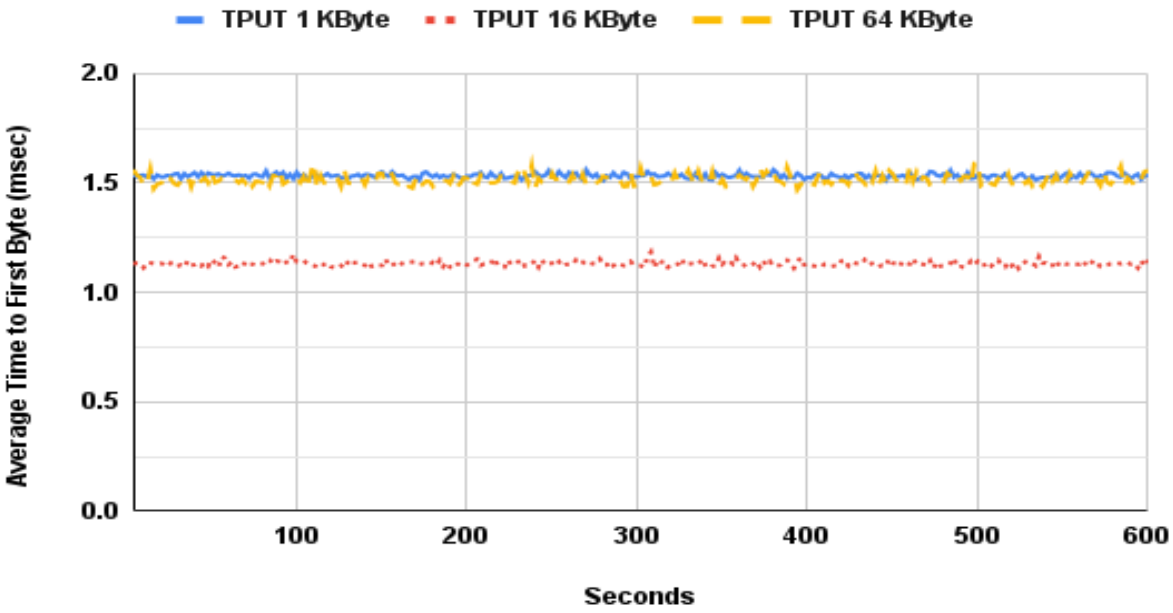


Sustainable inspected throughput of the DUT/SUT for HTTP transactions varying the HTTP response object size.

TCP/HTTP Transaction Latency Connections Per Second Sustained Phase

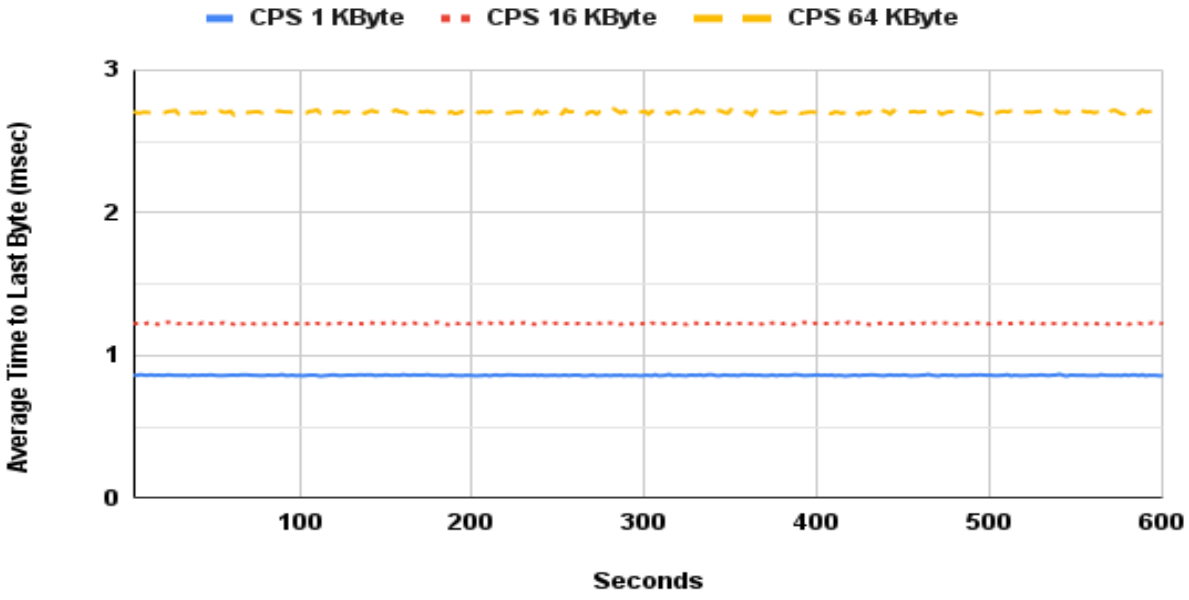


TCP/HTTP Transaction Latency Inspected Throughput Sustained Phase

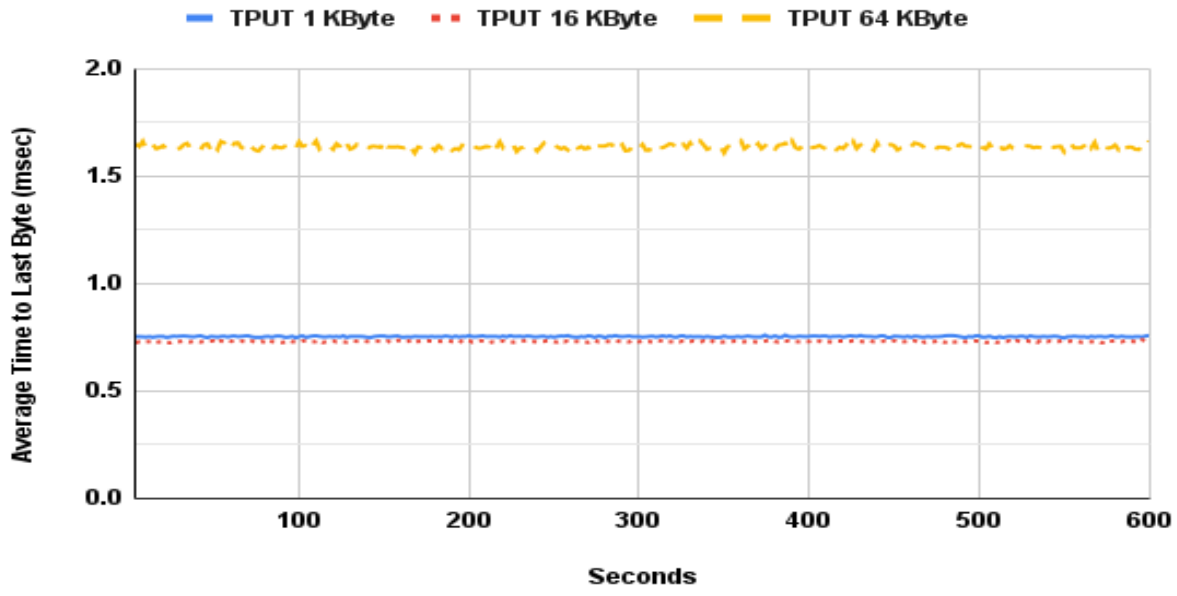


Average HTTP transaction latency time to first byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

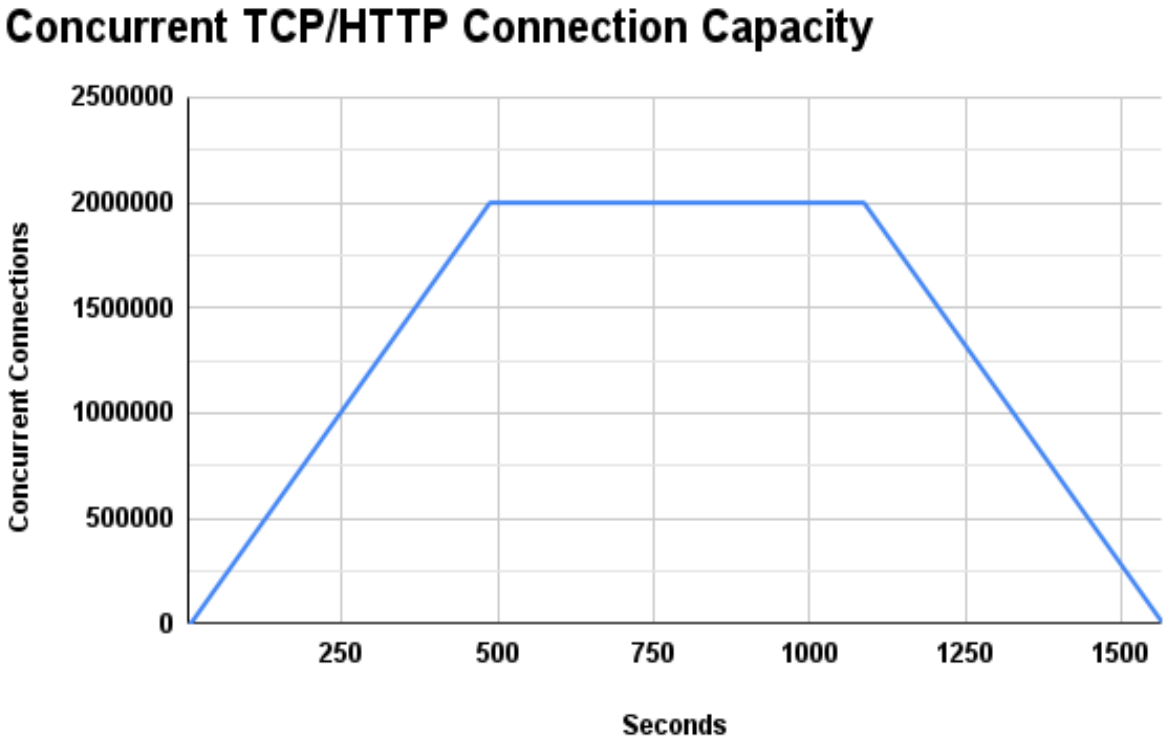
TCP/HTTP Transaction Latency Connections Per Second Sustained Phase



TCP/HTTP Transaction Latency Inspected Throughput Sustained Phase

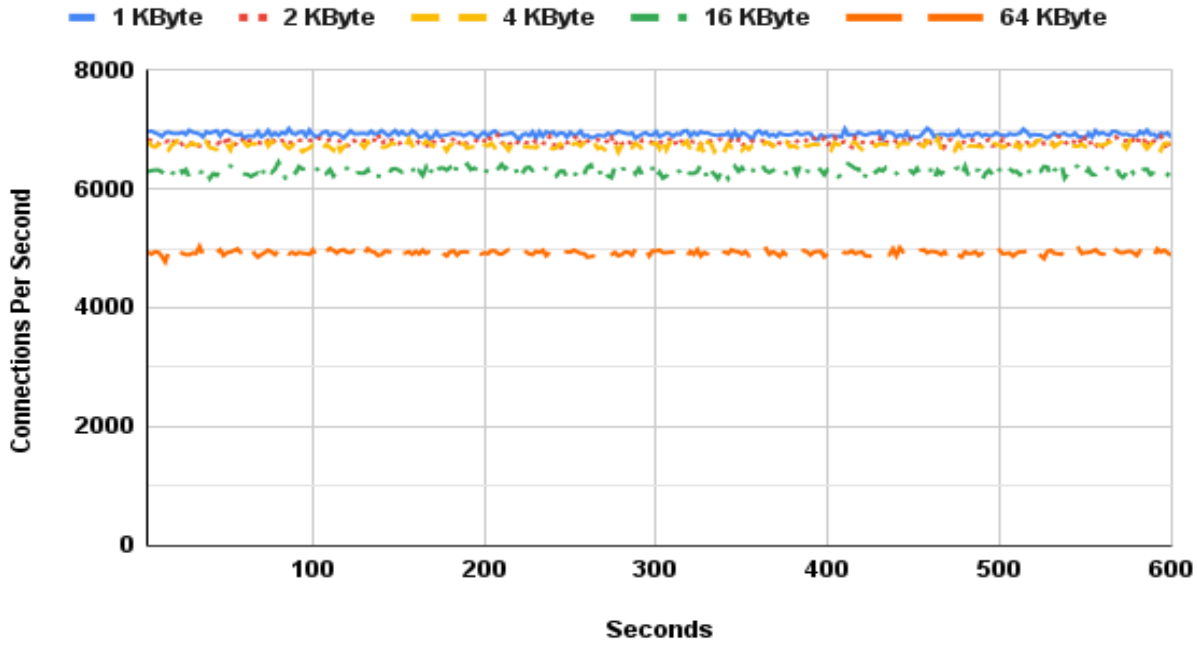


Average HTTP transaction latency time to last byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

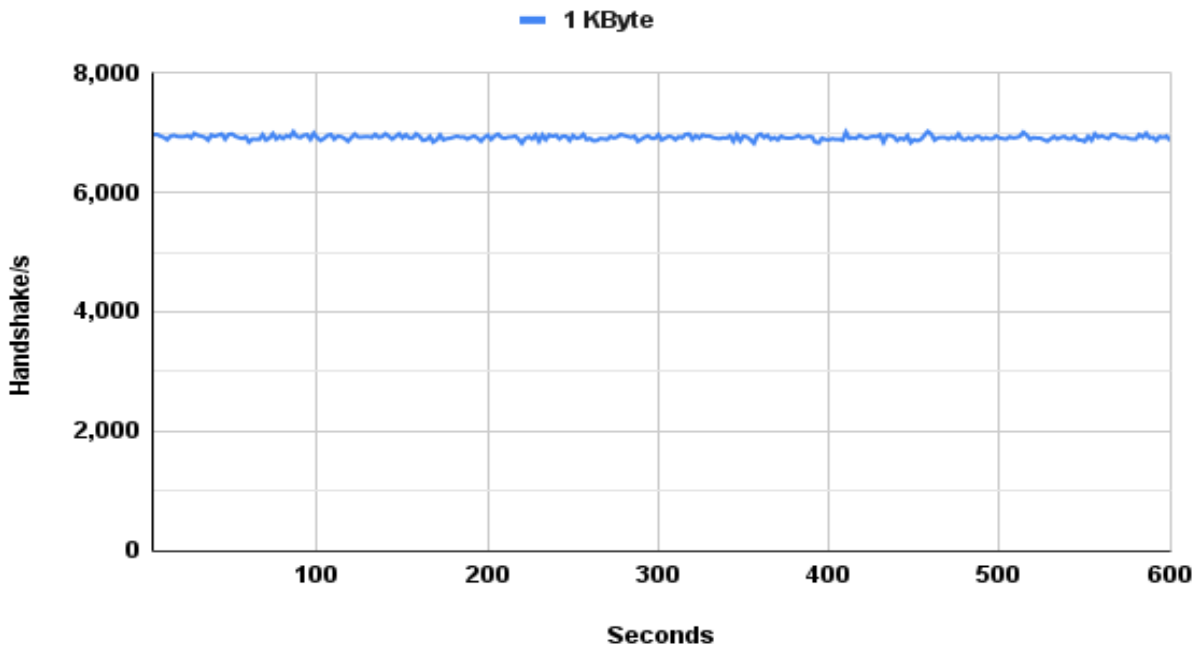


Number of concurrent TCP connections that the DUT/SUT sustains when using HTTP traffic.

TCP/HTTPS Connections Per Second Sustained Phase

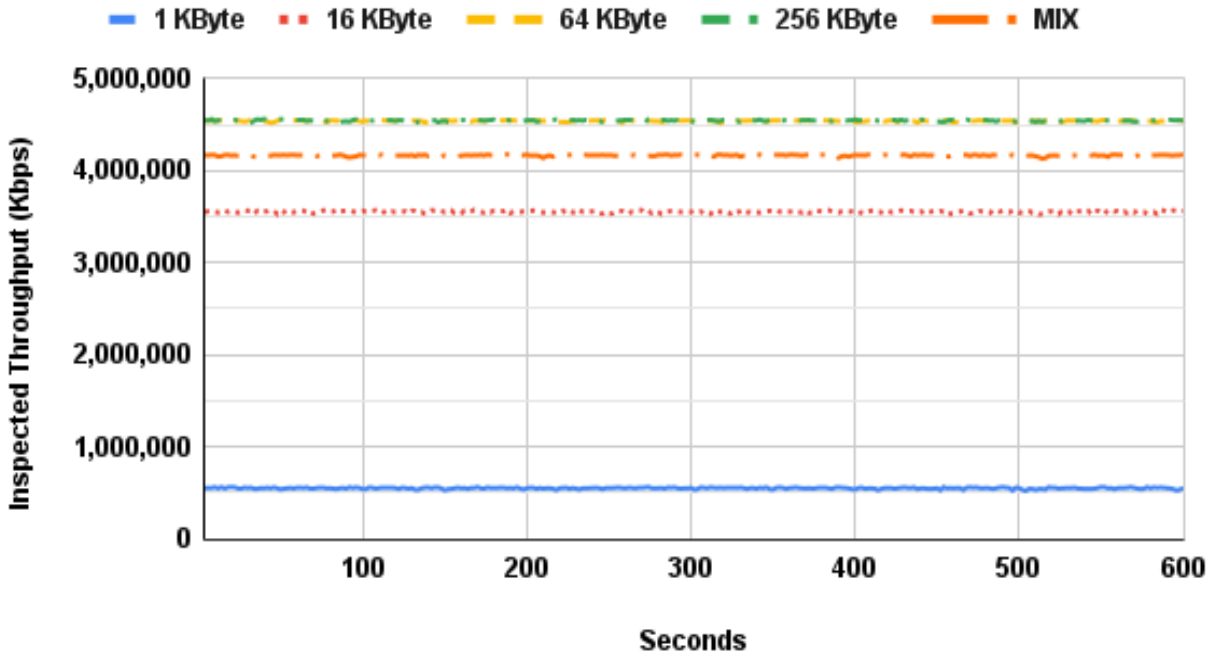


TCP/HTTPS TLS Handshake Rate Sustained Phase

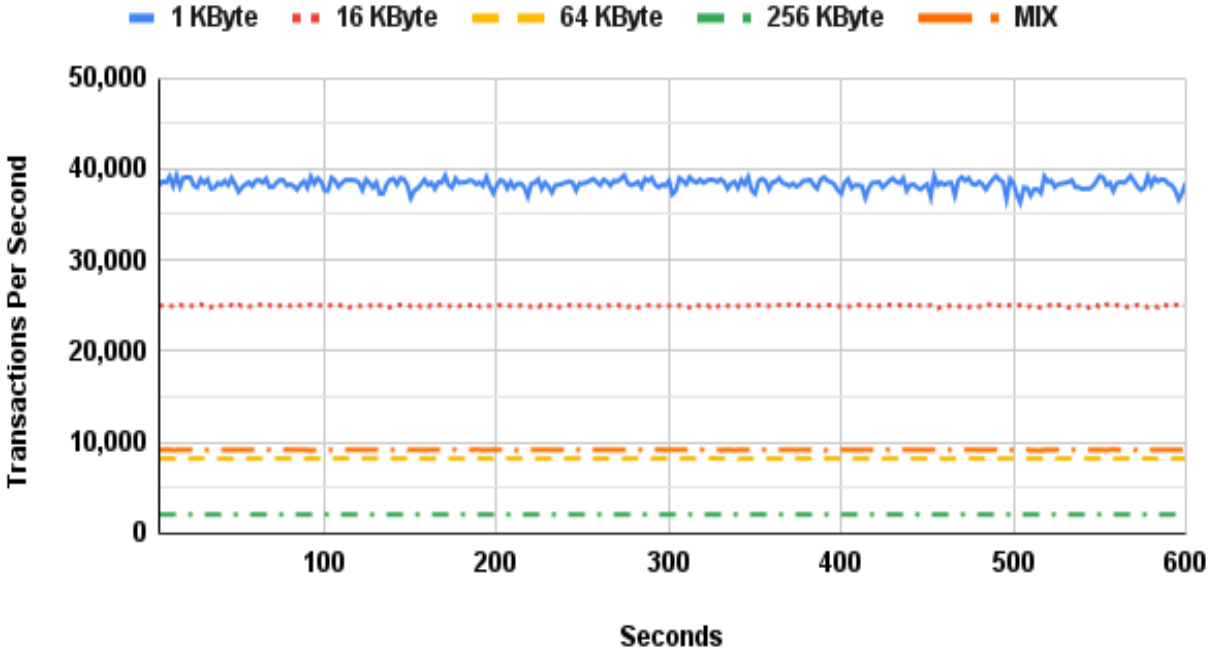


Sustainable SSL/TLS session establishment rate supported by the DUT/SUT under different throughput load conditions.

HTTPS Inspected Throughput Sustained Phase

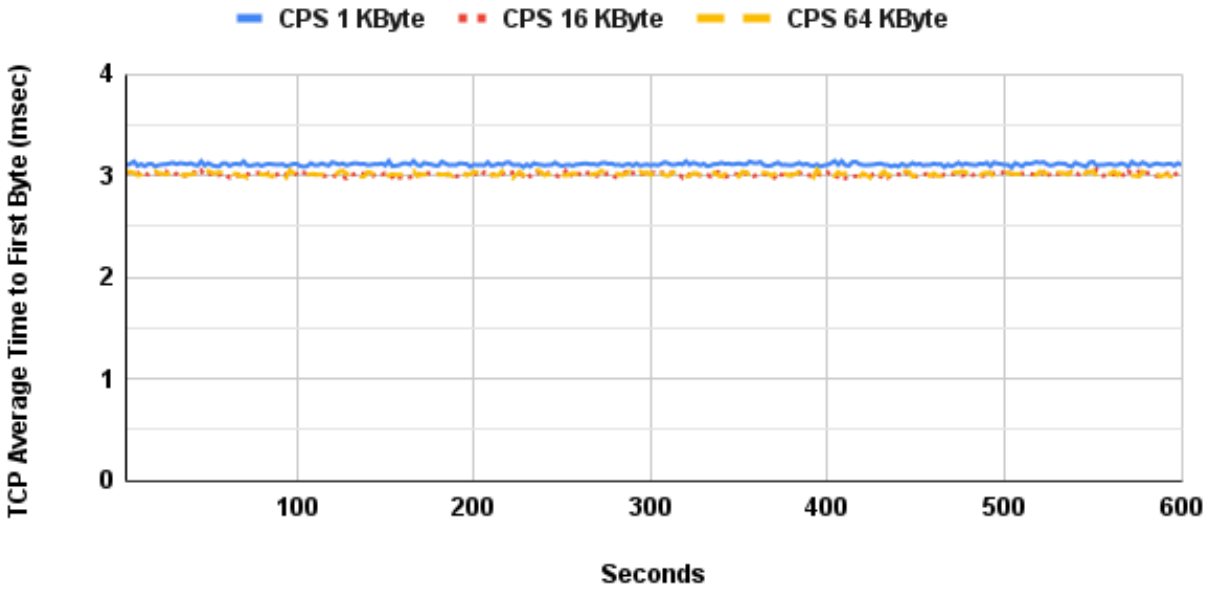


HTTPS Transactions Per Second Sustained Phase

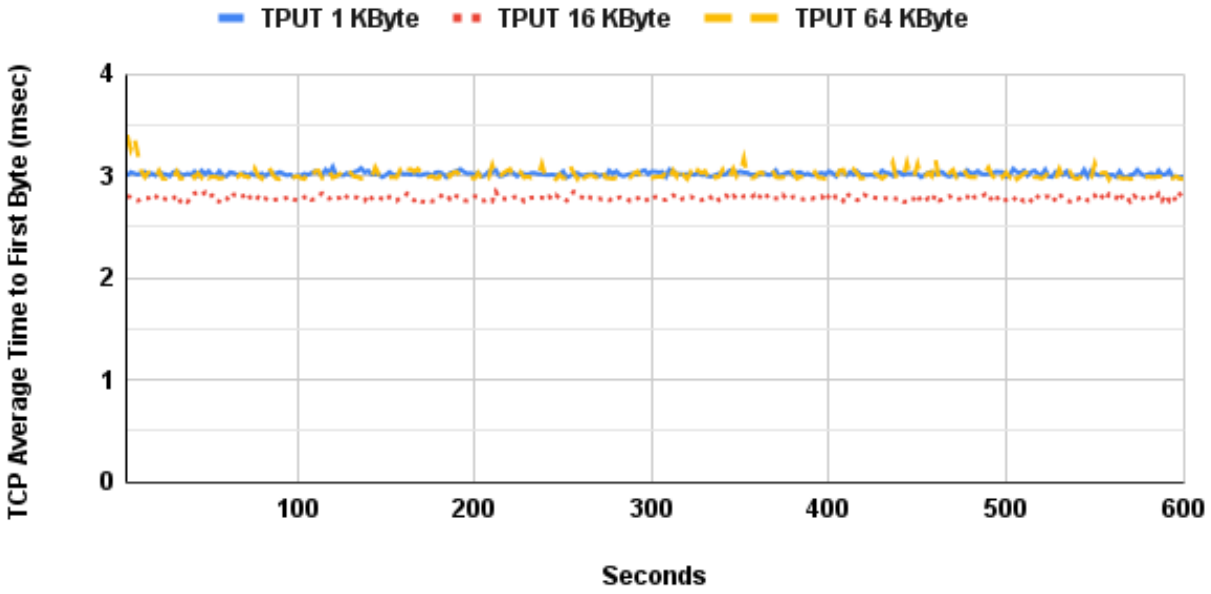


Sustainable inspected throughput of the DUT/SUT for HTTPS transactions varying the HTTPS response object size.

TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase

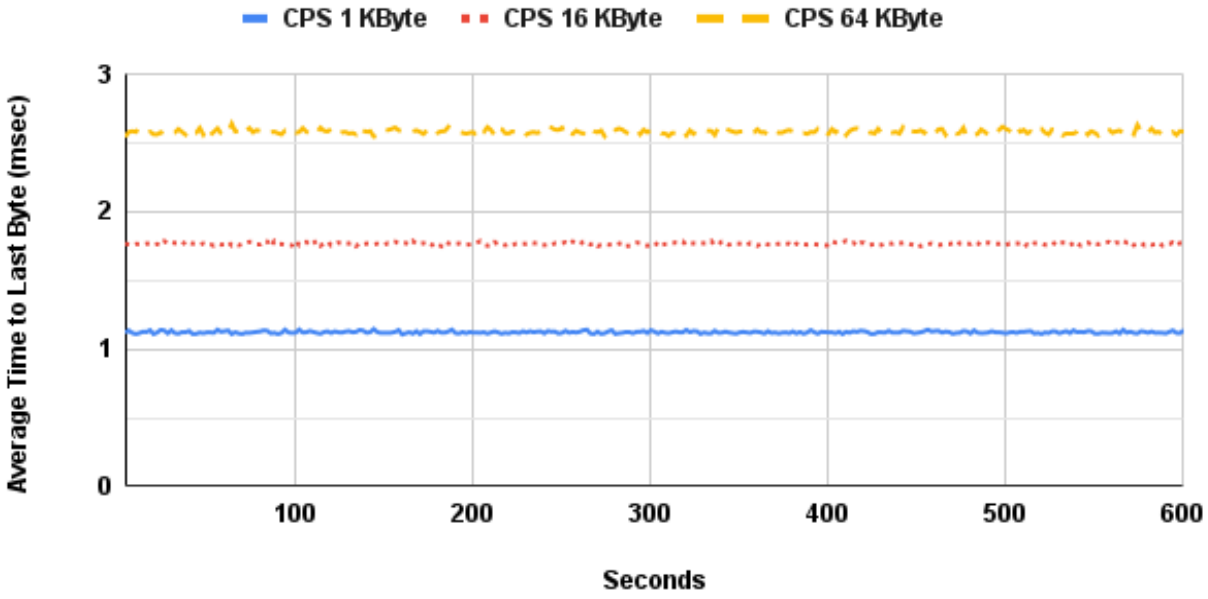


TCP/HTTPS Transaction Latency Inspected Throughput Sustained Phase

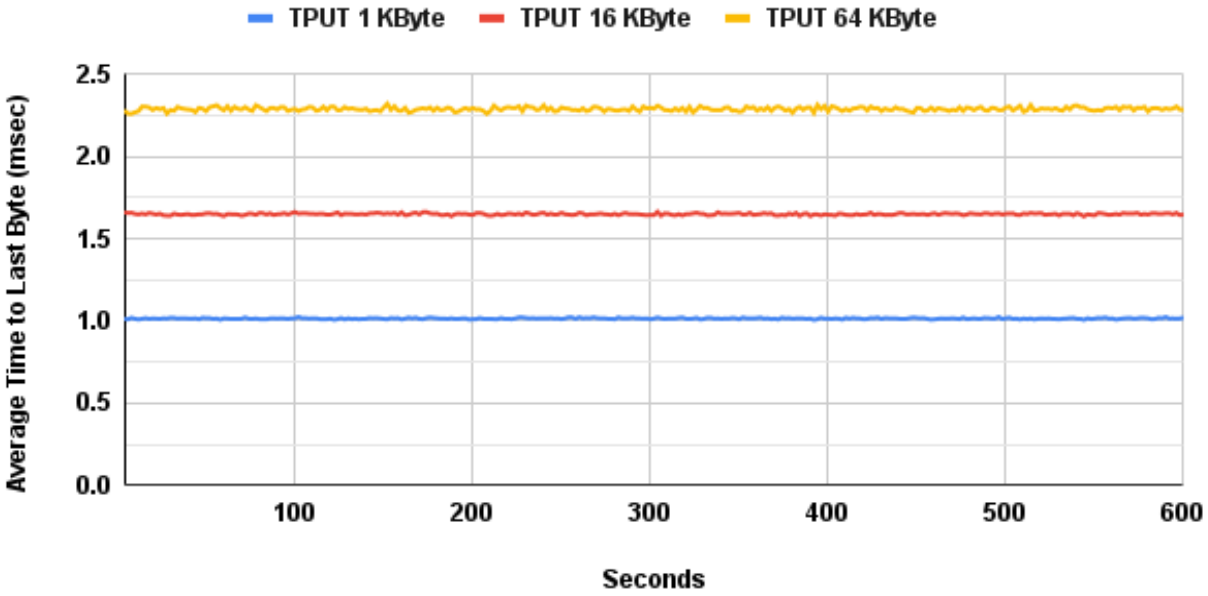


Average HTTPS transaction latency time to first byte under different HTTPS response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

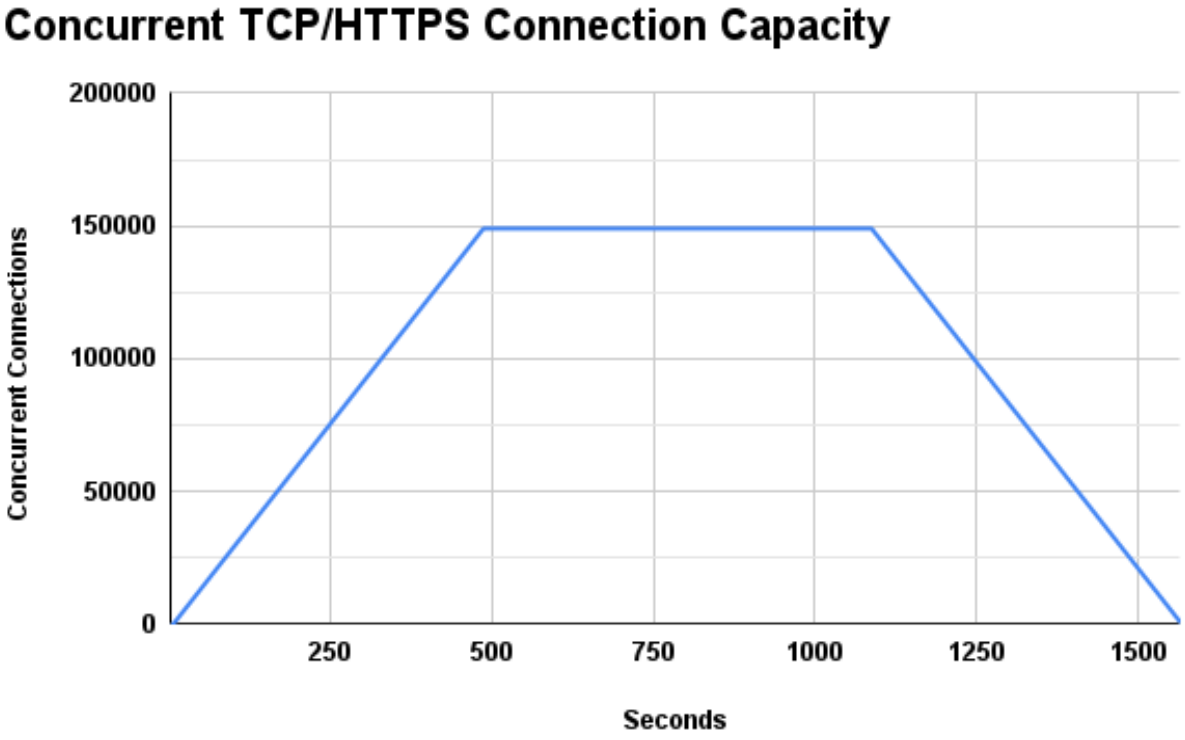
TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase



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	1,354	26
Private CVE	180	173	7
Malware	3,809	3,773	35
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)	3.44 (3,437,000)				3.02 (3,018,000)			
	TPS	14,292				16,801			
	CVE	Unique CVEs	Scenarios total	Blocked	Not Blocked	Unique CVEs	Scenarios total	Blocked	Not Blocked
		50	500	500	0	50	500	500	0