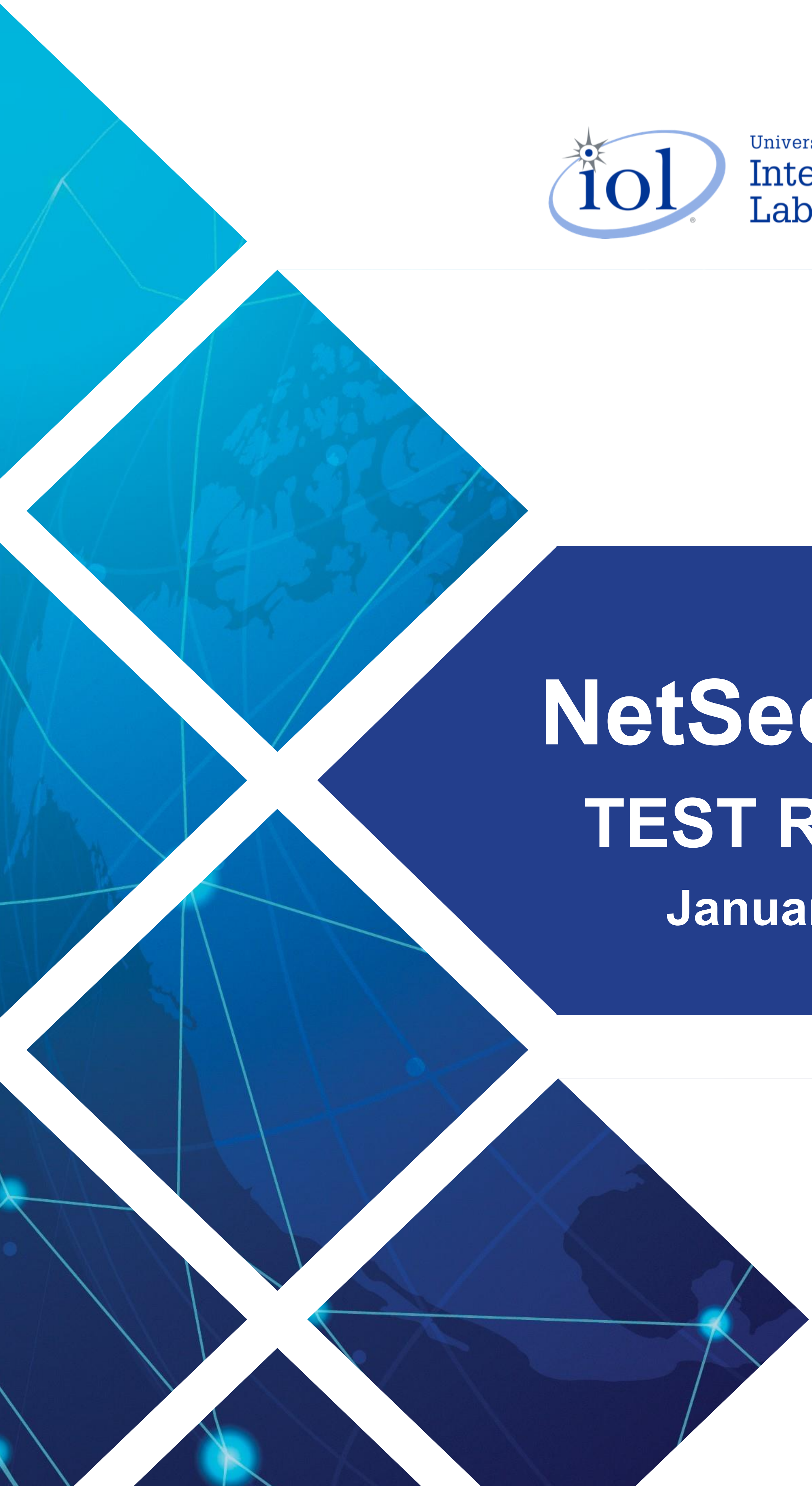
University of New Hampshire
InterOperability
Laboratory



NetSecOPEN

TEST REPORT

January 2025

www.iol.unh.edu

CATHERINE CURTIS
TREND MICRO, INC.
CATHERINE_CURTIS@TRENDMICRO.COM

DEVICE AND TEST PLAN INFORMATION	
Device Under Test (DUT)	TippingPoint 8600TXE
Test Specification/Suite	Benchmarking Methodology for Network Security Device Performance RFC 9411
UNH-IOL Test Result ID	39198

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.		Christopher Brown (March 12, 2025)

TESTING NOTES

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

NOTES
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). The DUT/SUT requires importing server(s) certificates and private keys to perform TLS-Inspection. These certificates and private keys could not be provided. 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. Section 7.1, Application Traffic Mixes reached ~98% of the test tools CPU threshold. We were unable to further increase inspected throughput and application transactions per second on the device under test due to this. Therefore, due to limitations of the test tool, the device under test could theoretically sustain increased inspected throughput and application transactions per second. Section 7.5, Concurrent TCP/HTTP Connection Capacity reached the test tools maximum memory threshold. We were unable to further increase concurrent connections on the device under test due to this. Therefore, due to limitations of the test tool, the device under test could theoretically sustain increased concurrent TCP/HTTP connections. The device under test does not log on each individual flow unless there is a filter match. If we were to configure a generic logging filter with an action to “allow/permit” for the performance traffic the device under test would potentially miss vulnerabilities since traffic would match on the logging filter rather than an applicable filter for the vulnerability. The device under test is capable of logging when a vulnerability is detected, ssl-inspection decryption logs, any traffic subject to quarantine and reputation logs. The device under test specializes in detection and prevention of Command and Control (C&C) attacks. NetSecOPEN's 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. C&C attacks post-infection are currently not included in the scenarios tested. Trend Micro has requested we omit these pre-infection malware tests.

REVISION HISTORY

The following table contains a revision history for this report.

REVISION	DATE	AUTHOR	EXPLANATION
1.0	01/31/25	Chris Brown	Initial version
2.0	02/14/25	Chris Brown	Added testing note regarding omission of malware set. Added footnote for Sections 7.1 and 7.5.
3.0	03/12/25	Chris Brown	Added clarification to report notes regarding Sections 7.1 and 7.5.

DEVICE INFORMATION

COMPONENT	DESCRIPTION
Device Name	TippingPoint 8600TXE
UNH-IOL Device Identification Number	FW-TRENDMIC-0000031219
Device Model	8600TXE
Device Firmware	TOS 6.3.0.13244
Digital Vaccine	4.0.0.9956
Auxiliary DV's	Malware 3.7.0.2009
Controller Name	TippingPoint Security Management System
Controller Model	Security Management System
Controller Firmware	6.3.0.207000.1
Performance Interfaces Tested	Slot 1 Ports 1,2,3,4
Performance Interfaces Speed	40G
Security Effectiveness Interfaces Tested	Slot 1 Ports 1,2,3,4
Security Effectiveness Interfaces Speed	40G

DEVICE ENABLED FEATURES

FEATURE	STATUS	
	ENABLED	DISABLED
TLS Inspection	✓	
Anti-Malware	✓	
Anti-Spyware	✓	
Anti-Botnet	✓	
Application Identification	✓	
Deep Packet Inspection (DPI)	✓	
Anti-Evasion	✓	
Logging and Reporting	✓	

TEST TOOL AND ENVIRONMENT INFORMATION

<table>
<tr><th>COMPONENT</th><th colspan="2">DESCRIPTION</th></tr>
<tr><td>Performance Test Equipment Vendor</td><td colspan="2">Keysight</td></tr>
<tr><td>Performance Hardware Name</td><td colspan="2">XGS2-HSL</td></tr>
<tr><td>Performance Hardware Firmware</td><td colspan="2">10.00.1000.14</td></tr>
<tr><td>Performance Hardware Interface Type</td><td colspan="2">40G</td></tr>
<tr><td>Performance Application Software Name</td><td colspan="2">BreakingPoint</td></tr>
<tr><td>Performance Application Software Version</td><td colspan="2">10.00.1.74</td></tr>
<tr><td>Performance Application and Threat Intelligence (ATI) Strikepack Version</td><td colspan="2">2024-13</td></tr>
<tr><td>Security Effectiveness Test Equipment Vendor</td><td colspan="2">Spirent</td></tr>
<tr><td>Security Effectiveness Hardware Name</td><td colspan="2">C200</td></tr>
<tr><td>Security Effectiveness Hardware Firmware</td><td colspan="2">5.50.4353</td></tr>
<tr><td>Security Effectiveness Hardware Interface Type</td><td colspan="2">40G</td></tr>
<tr><td>Security Effectiveness Application Software Name</td><td colspan="2">CyberFlood</td></tr>
<tr><td>Security Effectiveness Application Software Version</td><td colspan="2">24.6.1005</td></tr>
<tr><td>Client IP Subnet 1</td><td colspan="2">10.10.0.0/16</td></tr>
<tr><td>Server IP Subnet 1</td><td colspan="2">10.11.0.0/16</td></tr>
<tr><td>Client IP Subnet 2</td><td colspan="2">10.12.0.0/16</td></tr>
<tr><td>Server IP Subnet 2</td><td colspan="2">10.13.0.0/16</td></tr>
<tr><td rowspan="2">Traffic Distribution Ratio</td><td><b>IPv4</b></td><td><b>IPv6</b></td></tr>
<tr><td>100%</td><td>0%</td></tr>
<tr><td>Cipher Suite</td><td colspan="2">ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048</td></tr>
</table>

TESTBED SETUP

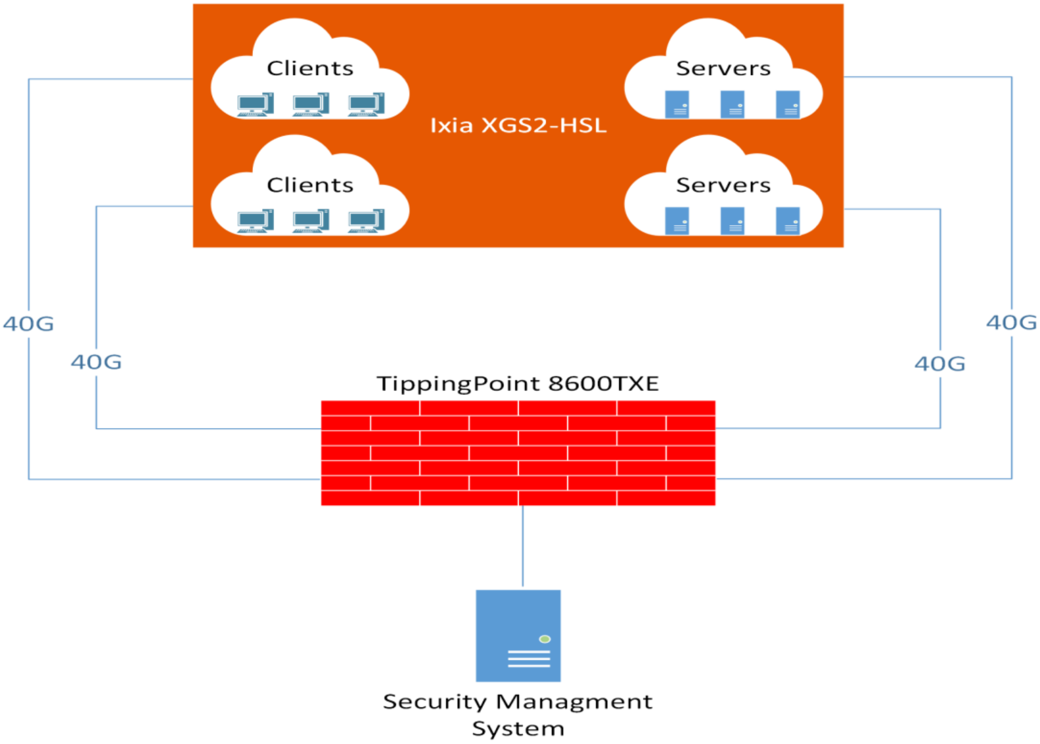


Figure 1: Topology with Performance Test Equipment Vendor

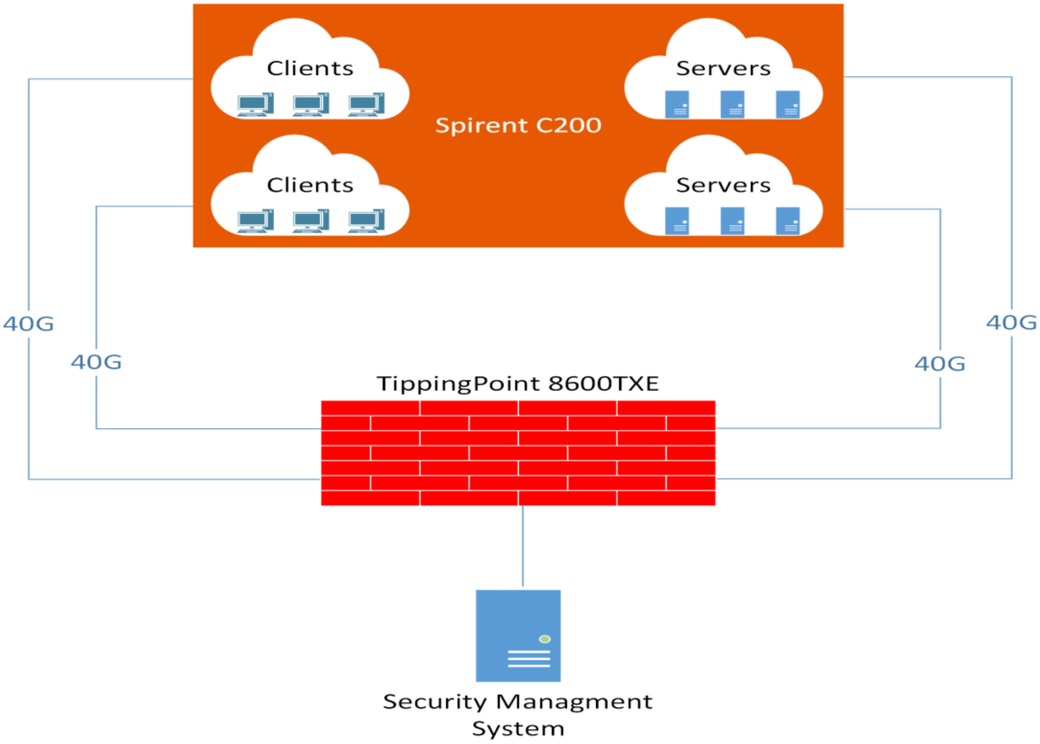


Figure 2: Topology with Security Effectiveness Test Equipment Vendor

SECURITY EFFECTIVENESS SUMMARY

SCENARIO	TOTAL	BLOCKED	ALLOWED	BLOCK RATE
Public CVE	1,380	1,354	26	98.12%
Private CVE	180	176	4	97.78%
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)	28.70 (28,696,000)	26.48 (26,485,000)
TPS	107,054	124,641
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)	30.16 (30,156,000) [1]	27.75 (27,747,000) [1]
	TPS	112,408 [1]	127,801 [1]

SECTION 7.2

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTP Connections Per Second	CPS	999,923	837,090	697,412	293,968	83,979

SECTION 7.3

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTP Inspected Throughput	TPUT Gbps (Kbps)	28.03 (28,031,000)	47.46 (47,460,000)	48.00 (48,009,000)	50.26 (50,269,000)	48.83 (48,829,000)
	TPS	1,679,864	329,916	86,866	23,000	107,440

[1] *Please refer to the testing notes section of this report regarding test case 7.1.

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)	0.068	0.076	0.076	0.097	0.119	0.202
	TTFB Minimum (msec)	0.062	0.070	0.071	0.095	0.116	0.184
	TTFB Maximum (msec)	0.073	0.080	0.082	0.098	0.121	0.222
	TTLB Average (msec)	0.139	0.273	0.825	0.140	0.280	0.857
	TTLB Minimum (msec)	0.129	0.260	0.793	0.137	0.275	0.817
	TTLB Maximum (msec)	0.146	0.290	0.860	0.141	0.284	0.903

SECTION 7.5

TEST CASE	KPI	1K
Concurrent TCP/HTTP Connection Capacity	CC	240,000,000 [2]

[2] *Please refer to the testing notes section of this report regarding test case 7.5.

SECTION 7.6

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTPS Connections Per Second	CPS	19,102	19,023	18,832	18,007	14,717
	HR	1K				
		19,102				

SECTION 7.7

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTPS Inspected Throughput	TPUT Gbps (Kbps)	2.52 (2,519,000)	17.32 (17,325,000)	28.91 (28,915,000)	39.08 (39,079,000)	30.80 (30,805,000)
	TPS	149,966	119,973	51,513	17,755	67,394

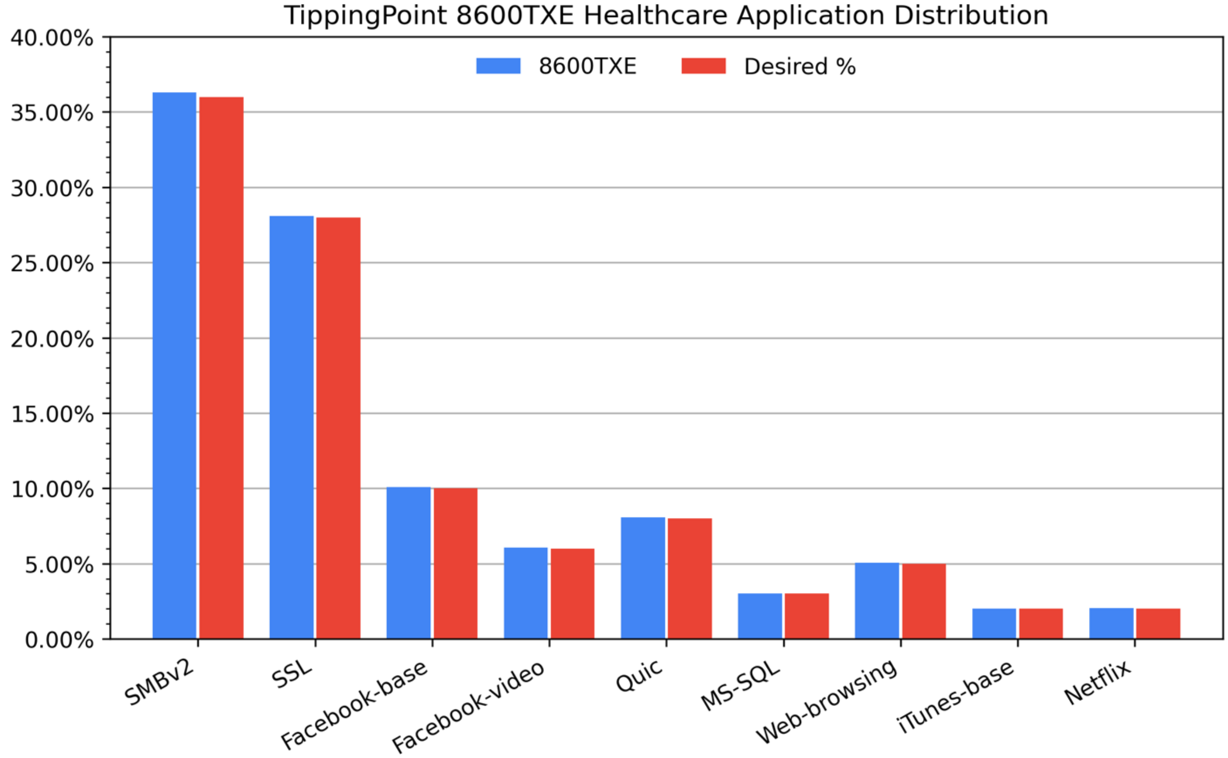
SECTION 7.8

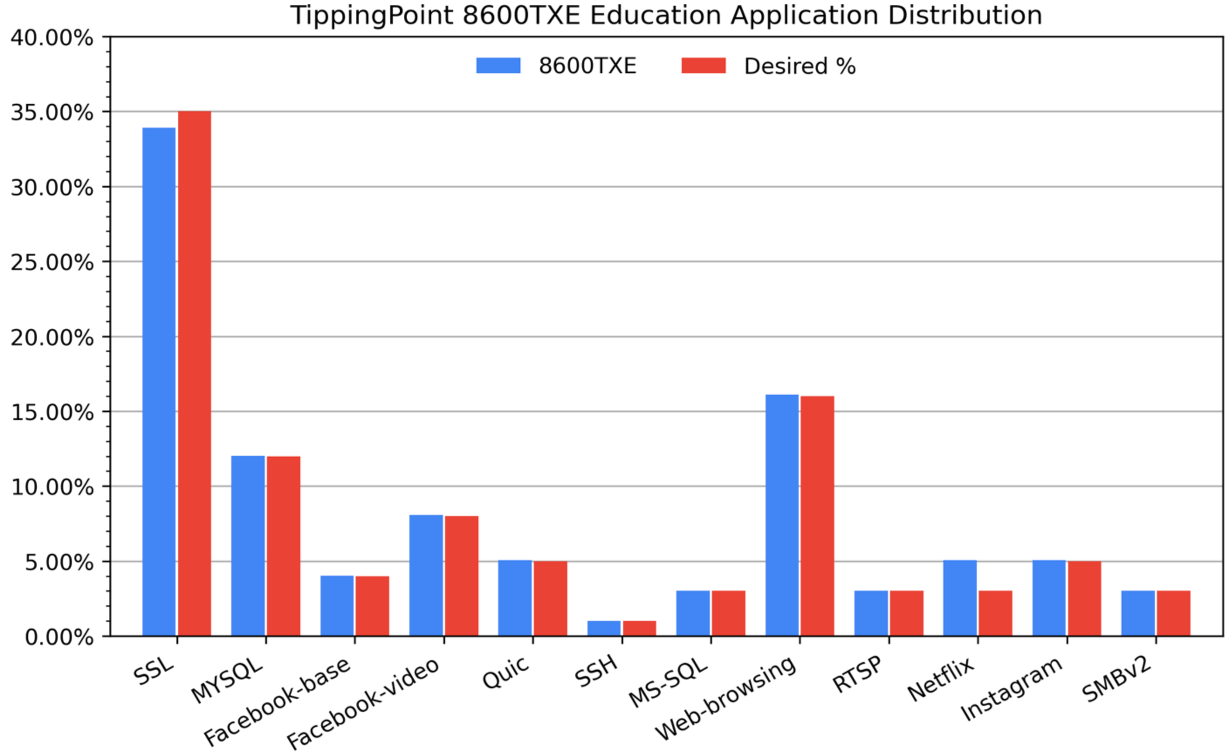
TEST CASE	KPI	CPS 1K	CPS 16K	CPS 64K	TPUT 1K	TPUT 16K	TPUT 64K
TCP/HTTPS Transaction Latency	TTFB Average (msec)	0.444	0.675	0.638	0.124	0.266	0.192
	TTFB Minimum (msec)	0.406	0.626	0.594	0.110	0.253	0.178
	TTFB Maximum (msec)	0.504	0.725	0.688	0.140	0.280	0.207
	TTLB Average (msec)	0.362	0.448	0.615	0.405	0.563	2.648
	TTLB Minimum (msec)	0.328	0.404	0.566	0.382	0.529	2.387
	TTLB Maximum (msec)	0.413	0.490	0.666	0.431	0.588	3.010

SECTION 7.9

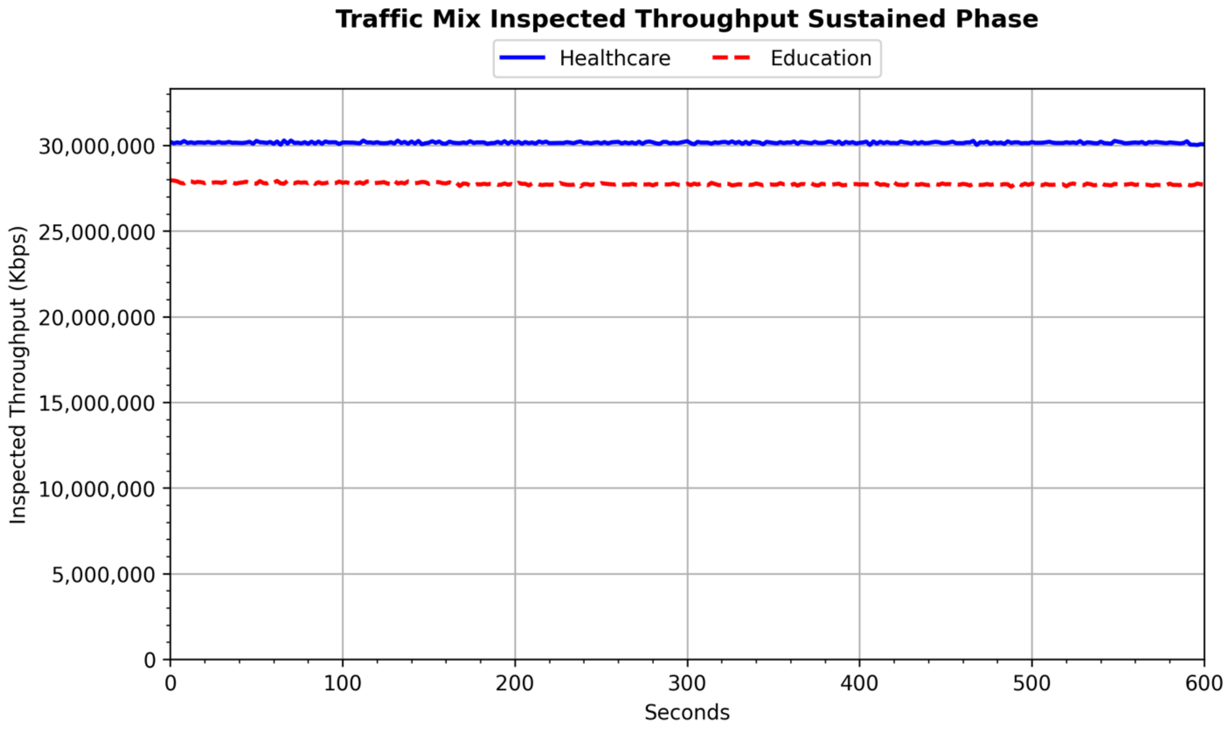
TEST CASE	KPI	1K
Concurrent TCP/HTTPS Connection Capacity	CC	250,000

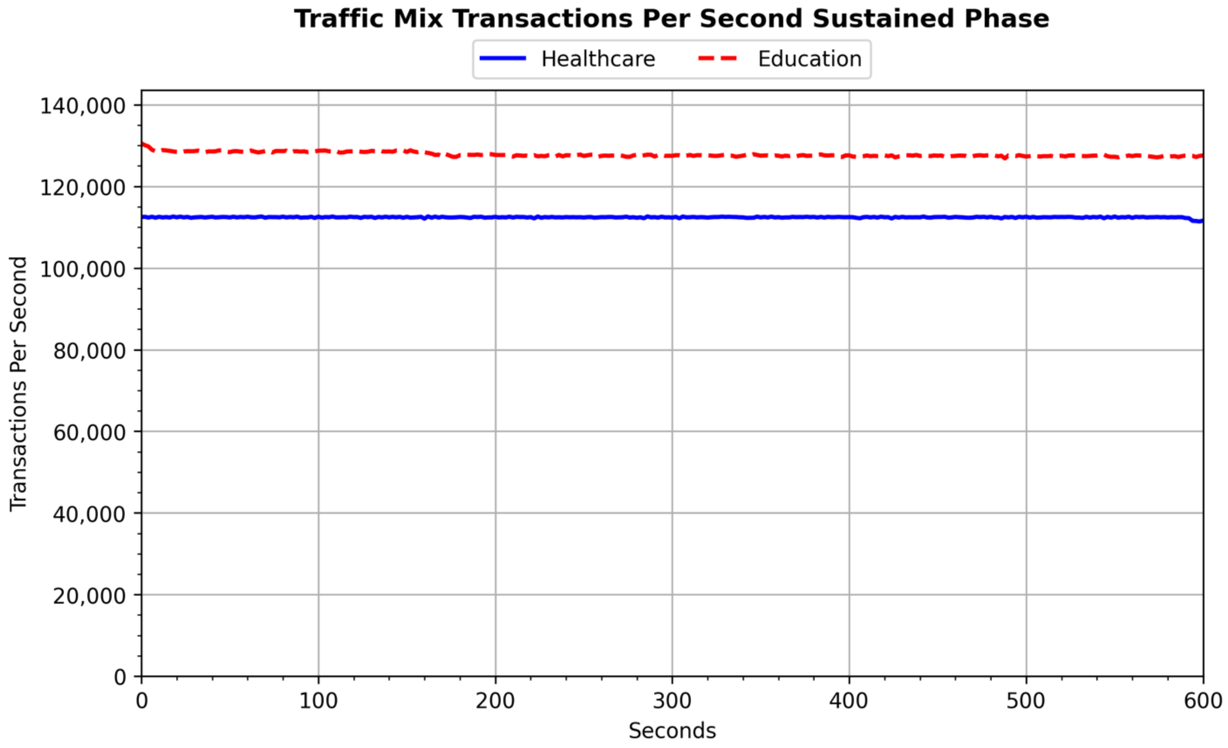
GRAPHS



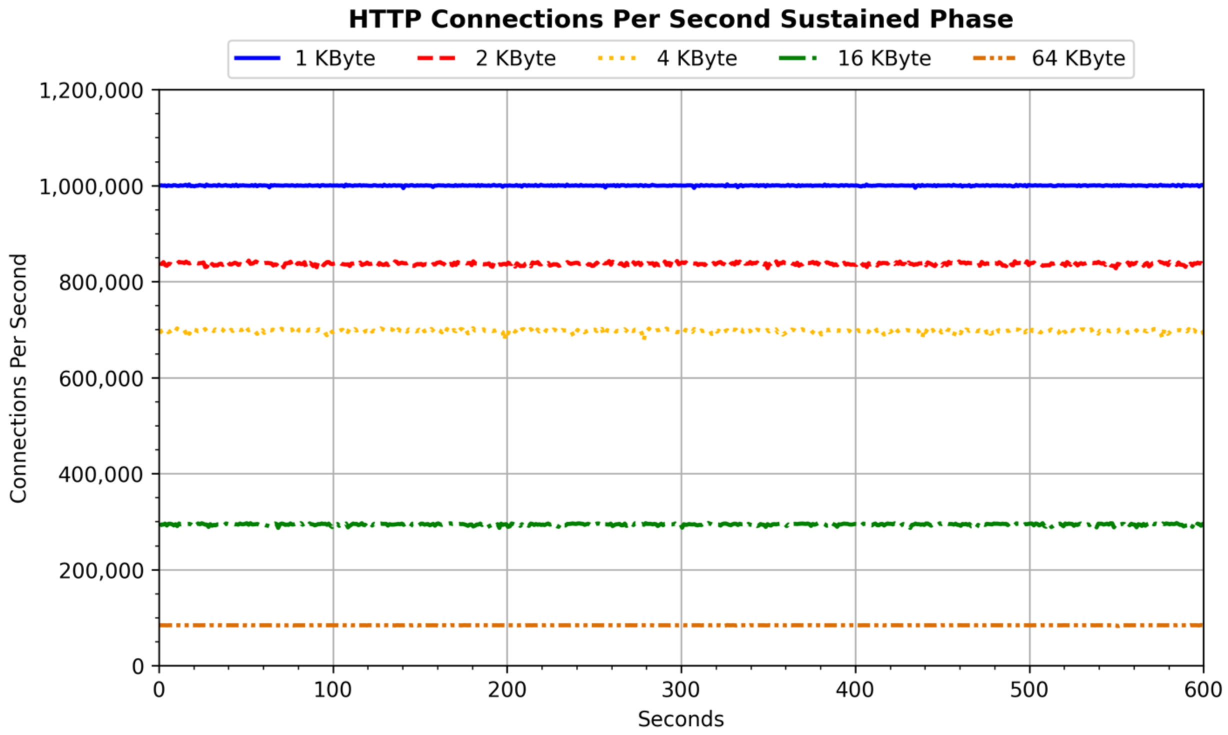


Comparison of desired Inspected Throughput and observed Inspected Throughput for each application within the traffic mixes.

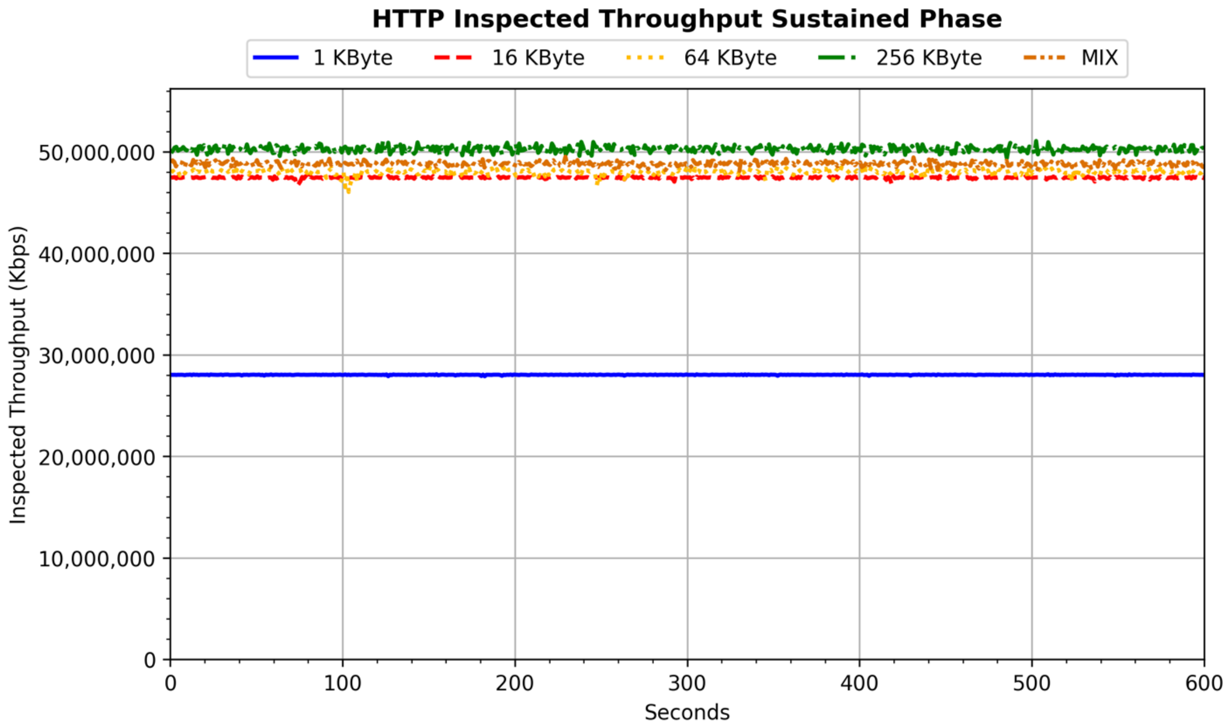


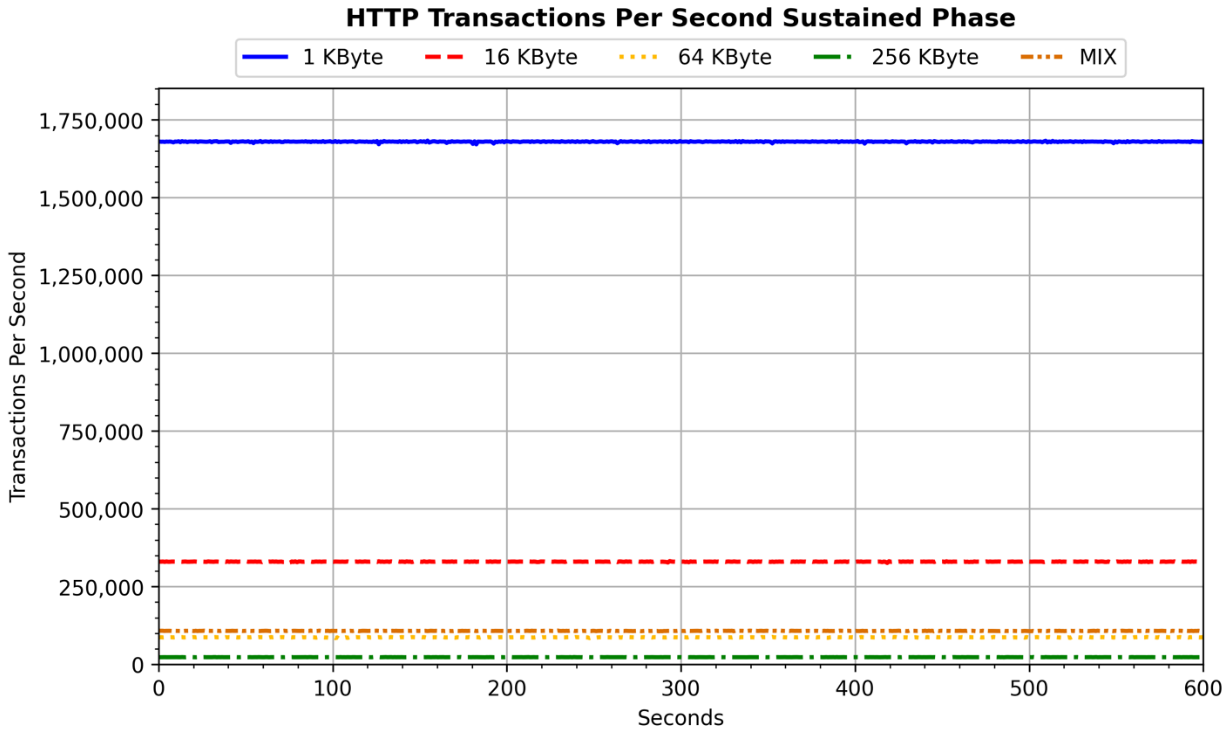


Sustainable inspected throughput of the DUT/SUT for Application Traffic Mixes.

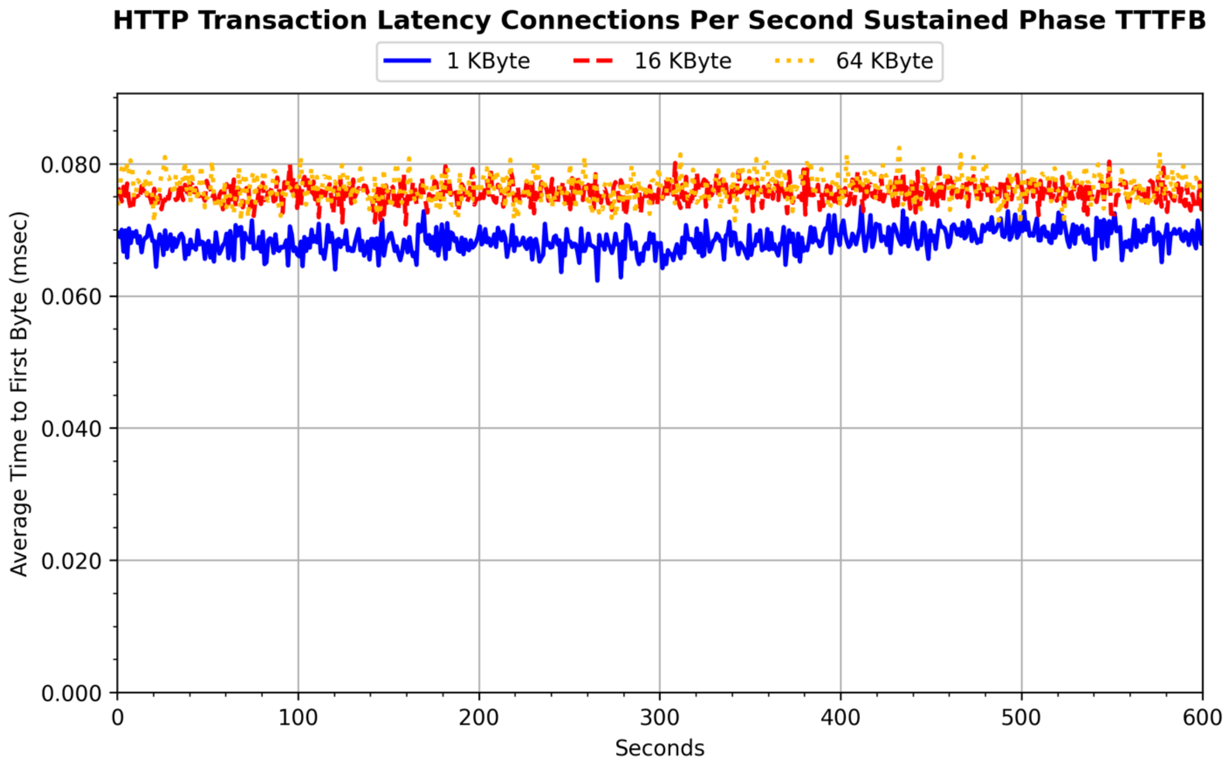


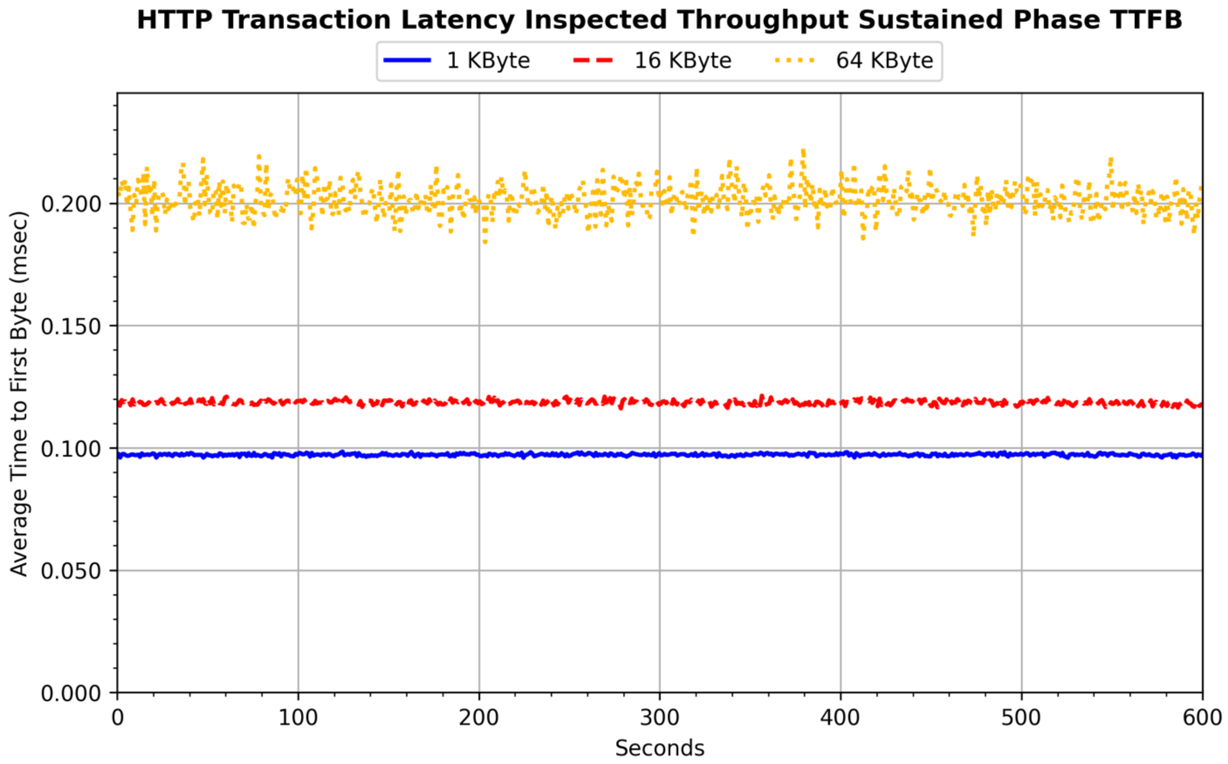
Sustainable TCP/HTTP connection establishment rate supported by the DUT/SUT under different throughput load conditions.



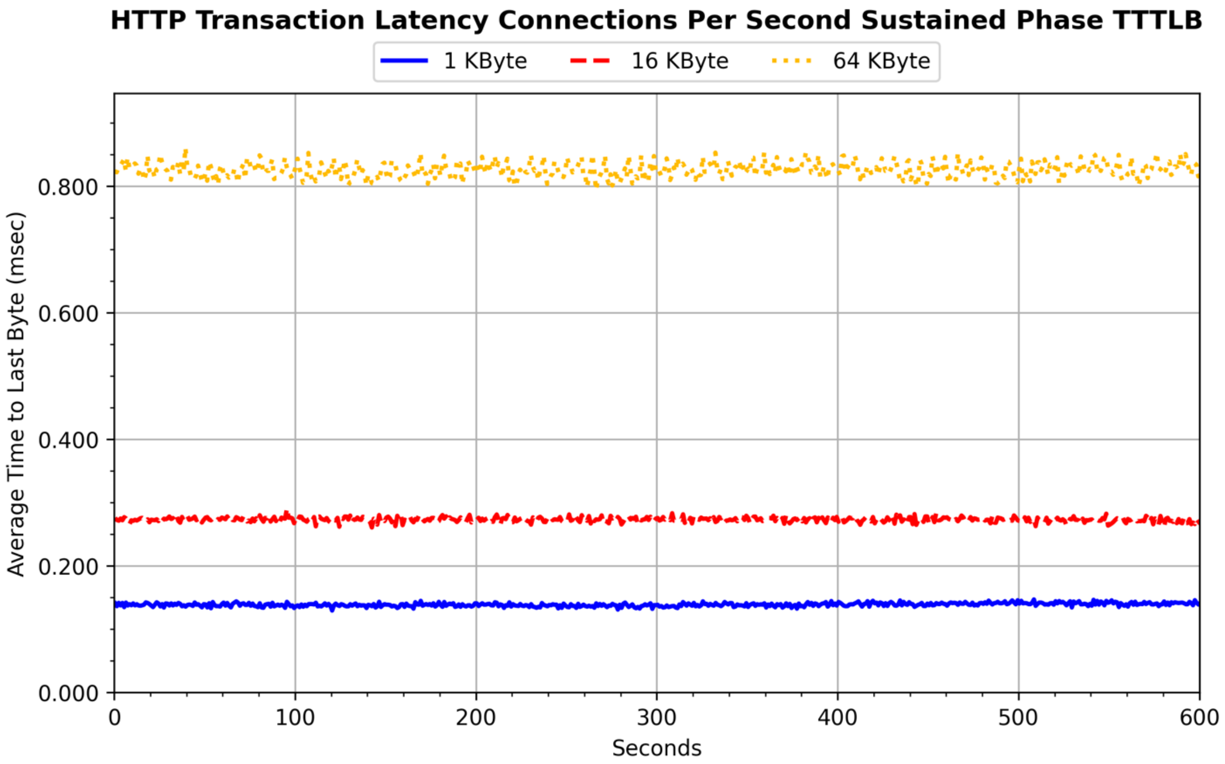


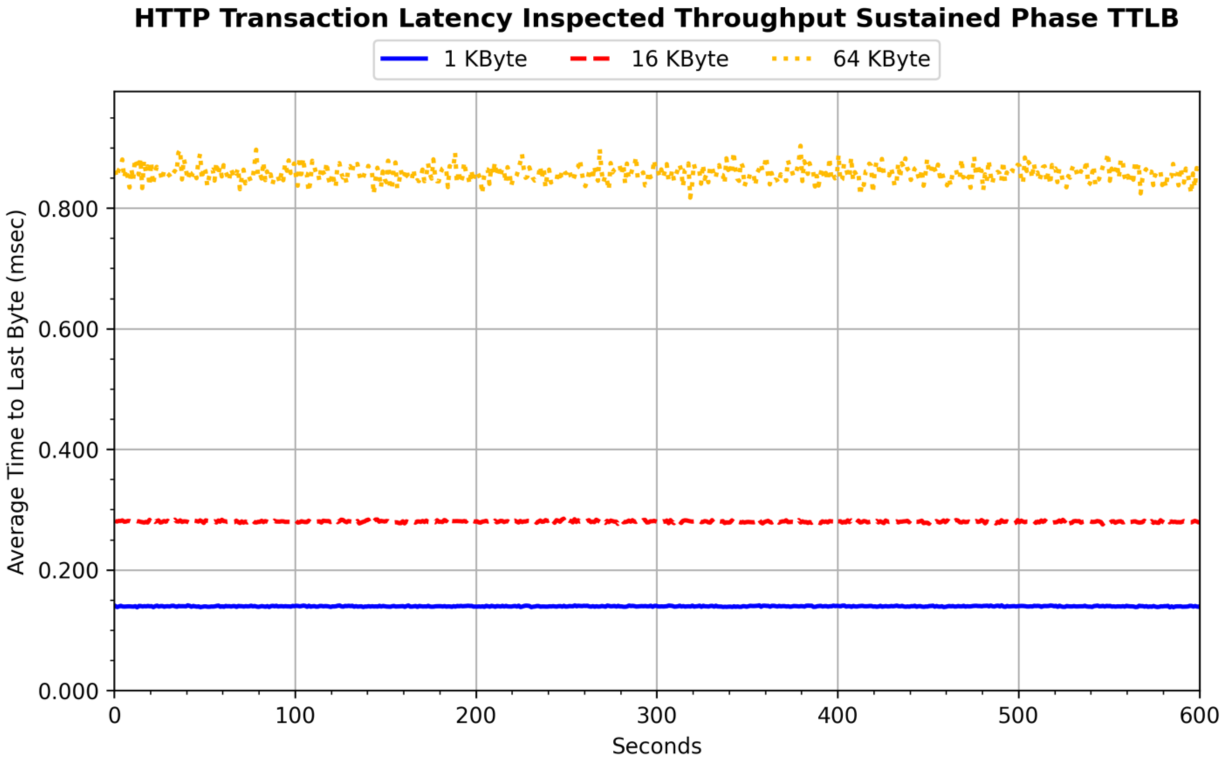
Sustainable inspected throughput of the DUT/SUT for HTTP transactions varying the HTTP response object size.



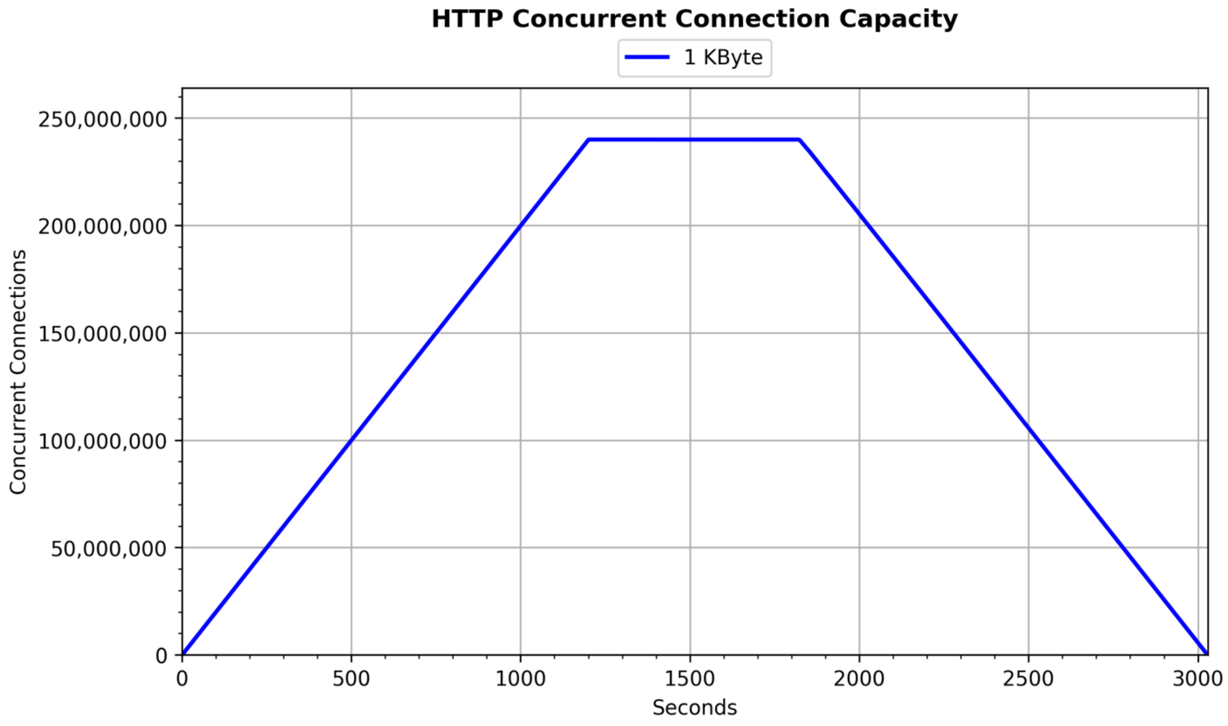


Average HTTP transaction latency time to first byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

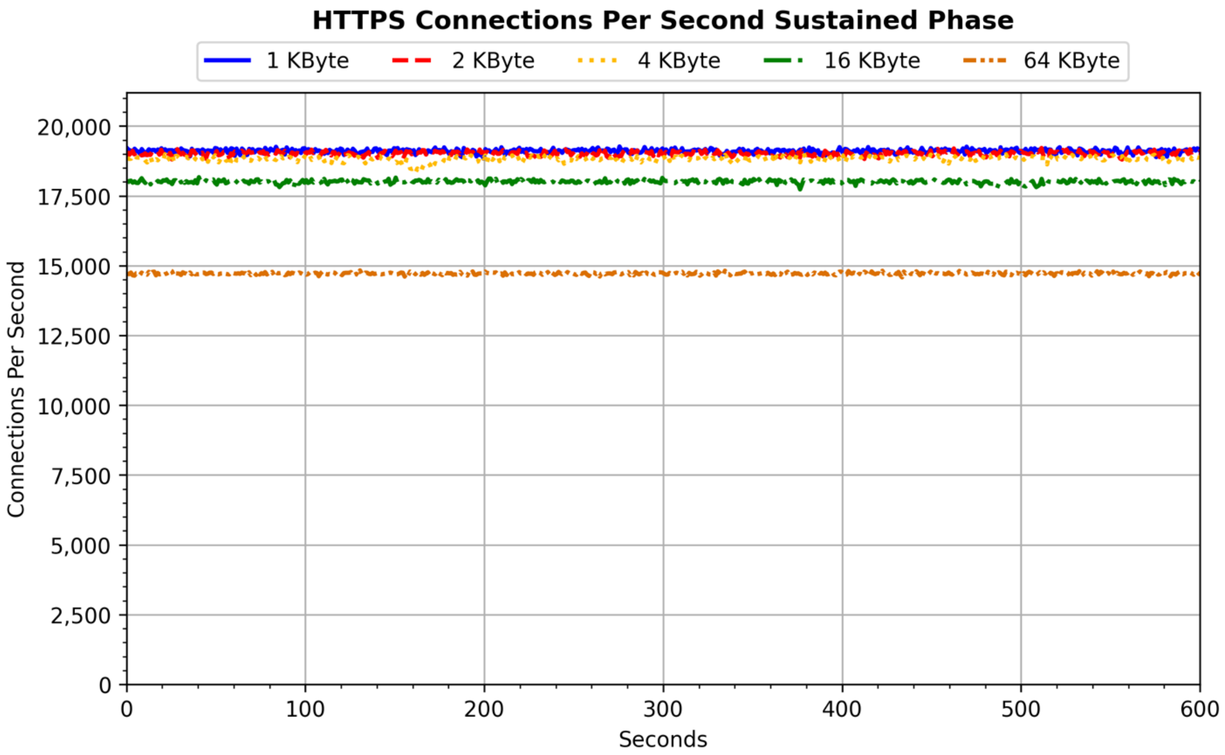


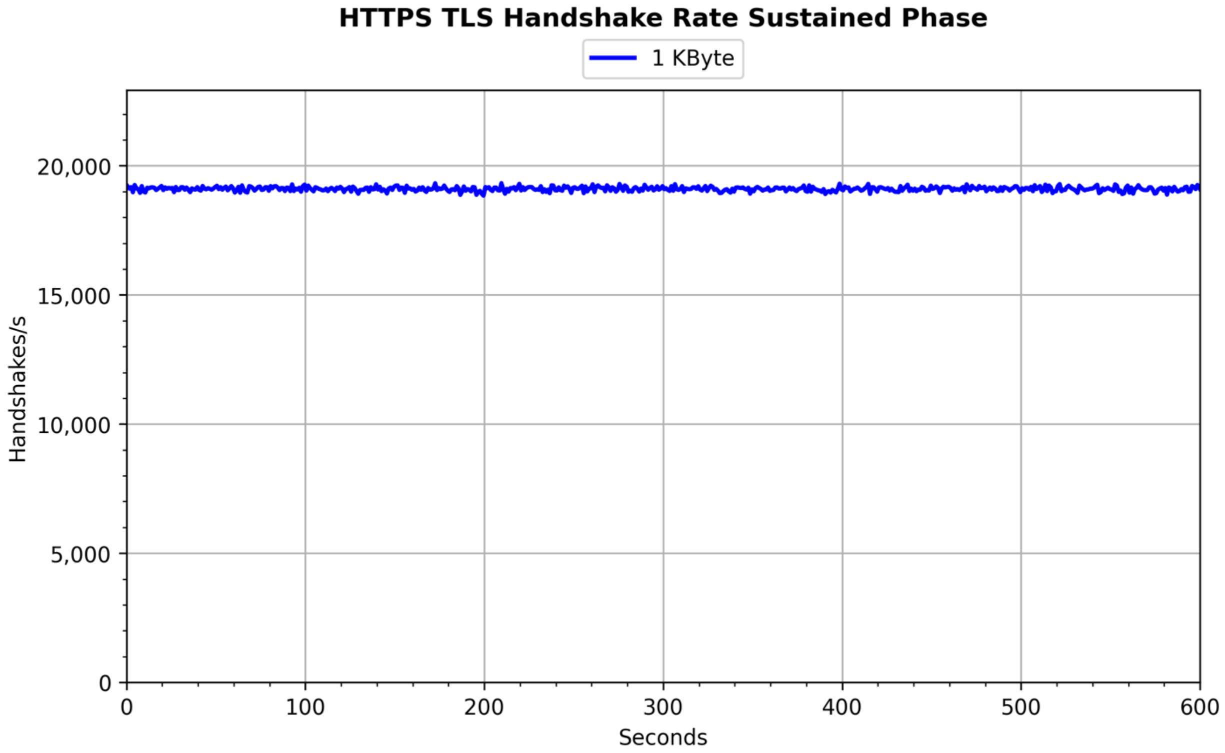


Average HTTP transaction latency time to last byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

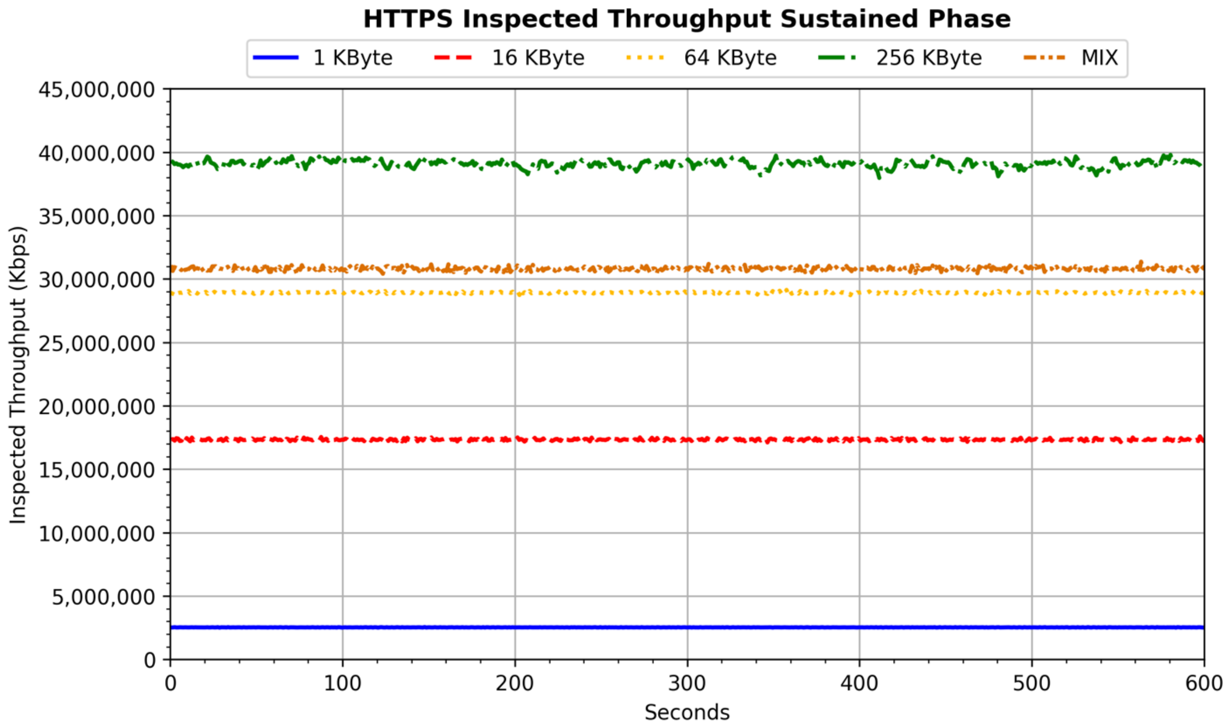


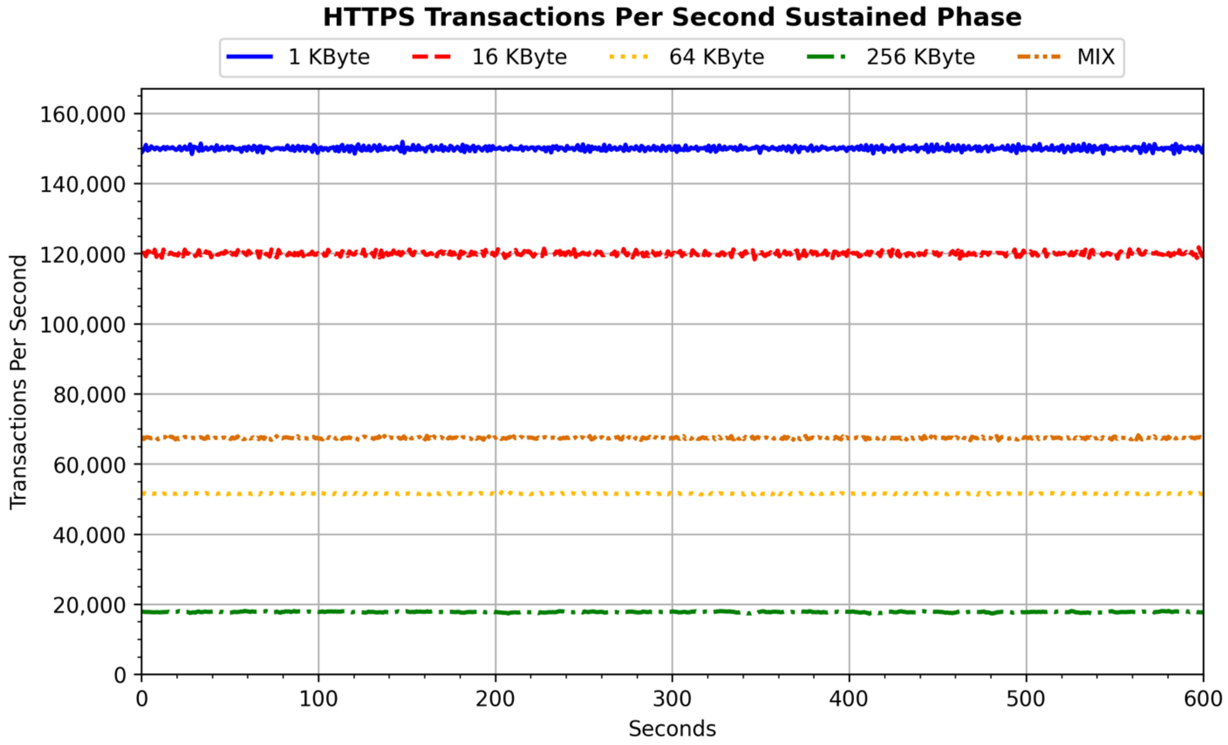
Number of concurrent TCP connections that the DUT/SUT sustains when using HTTP traffic.



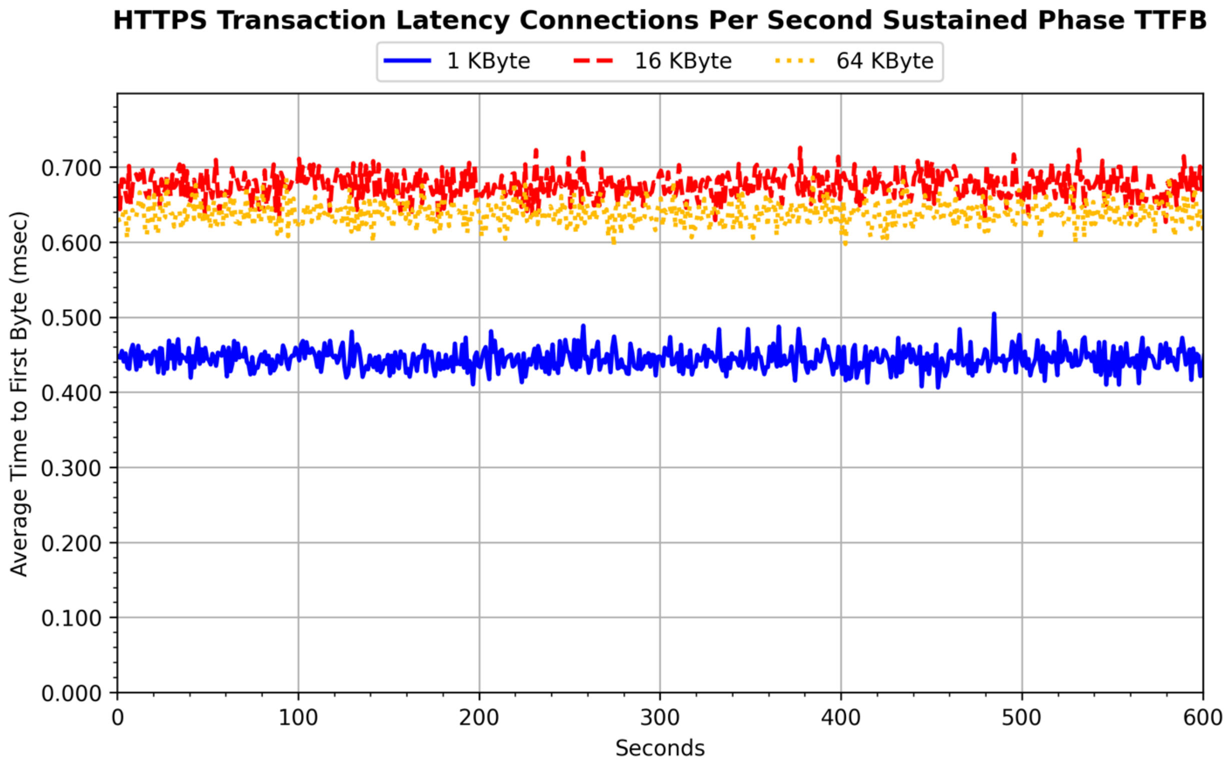


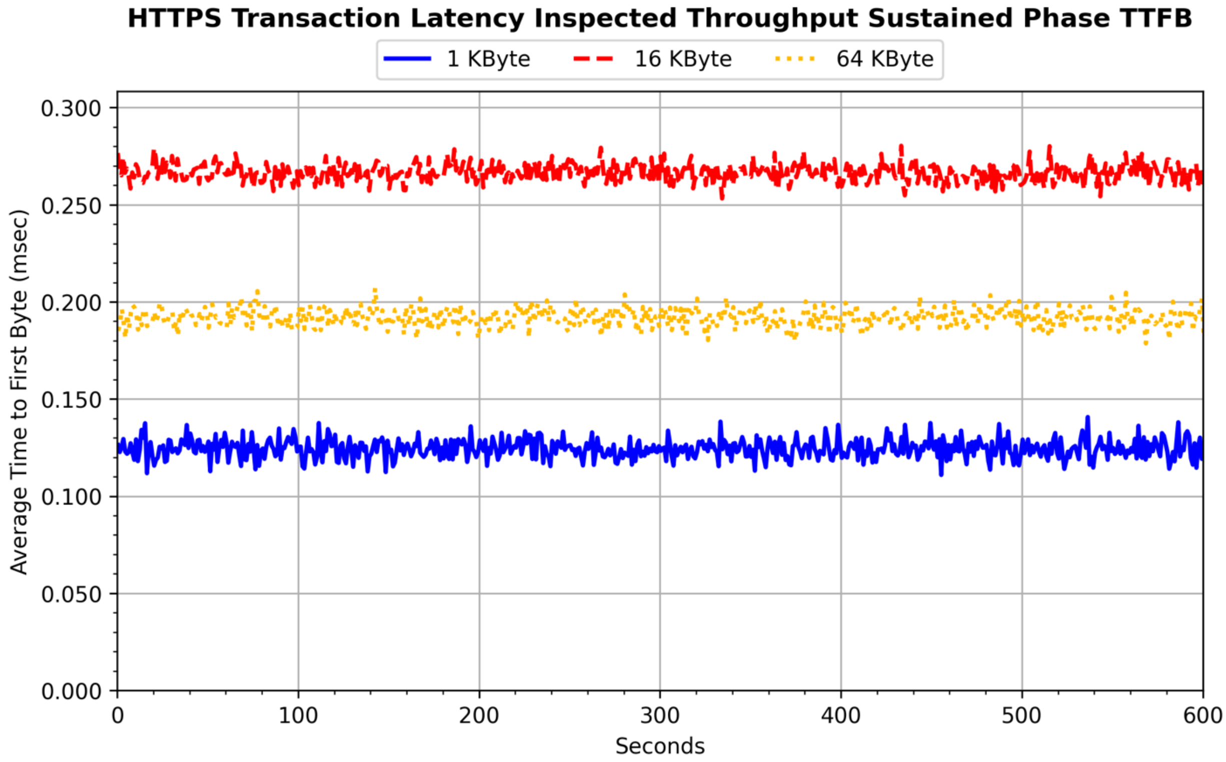
Sustainable SSL/TLS session establishment rate supported by the DUT/SUT under different throughput load conditions.



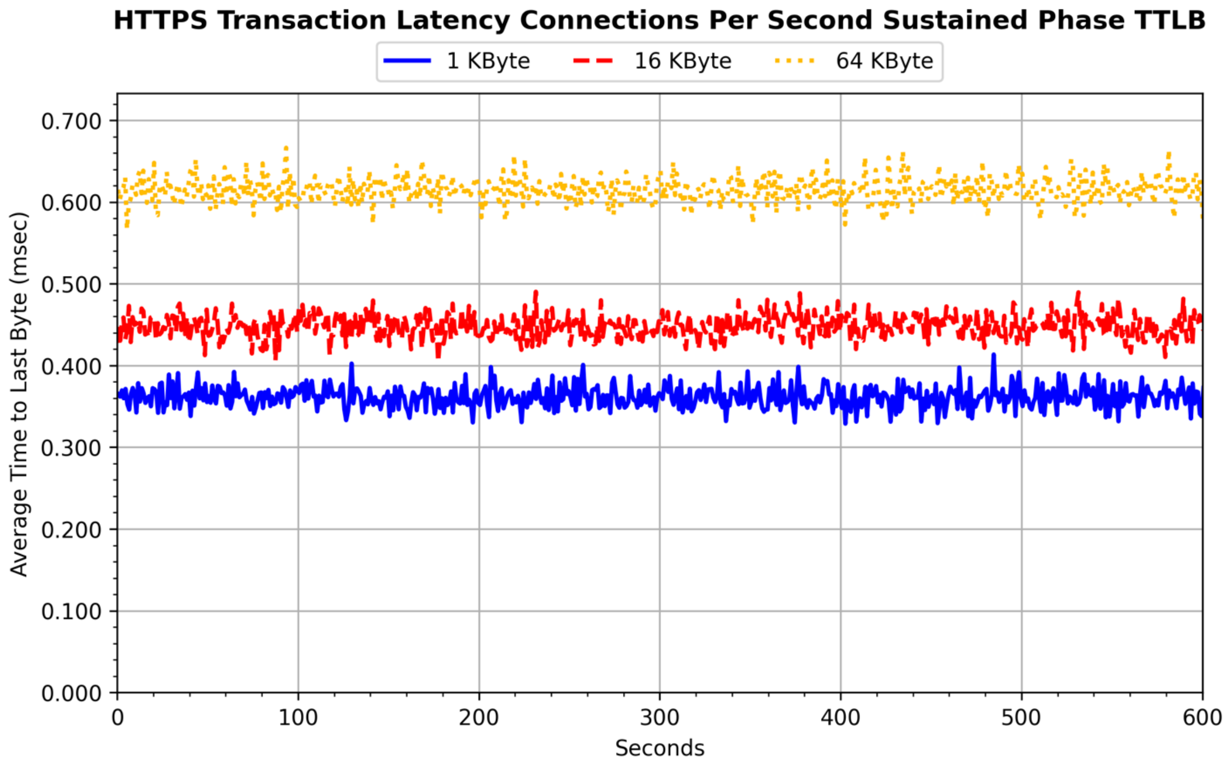


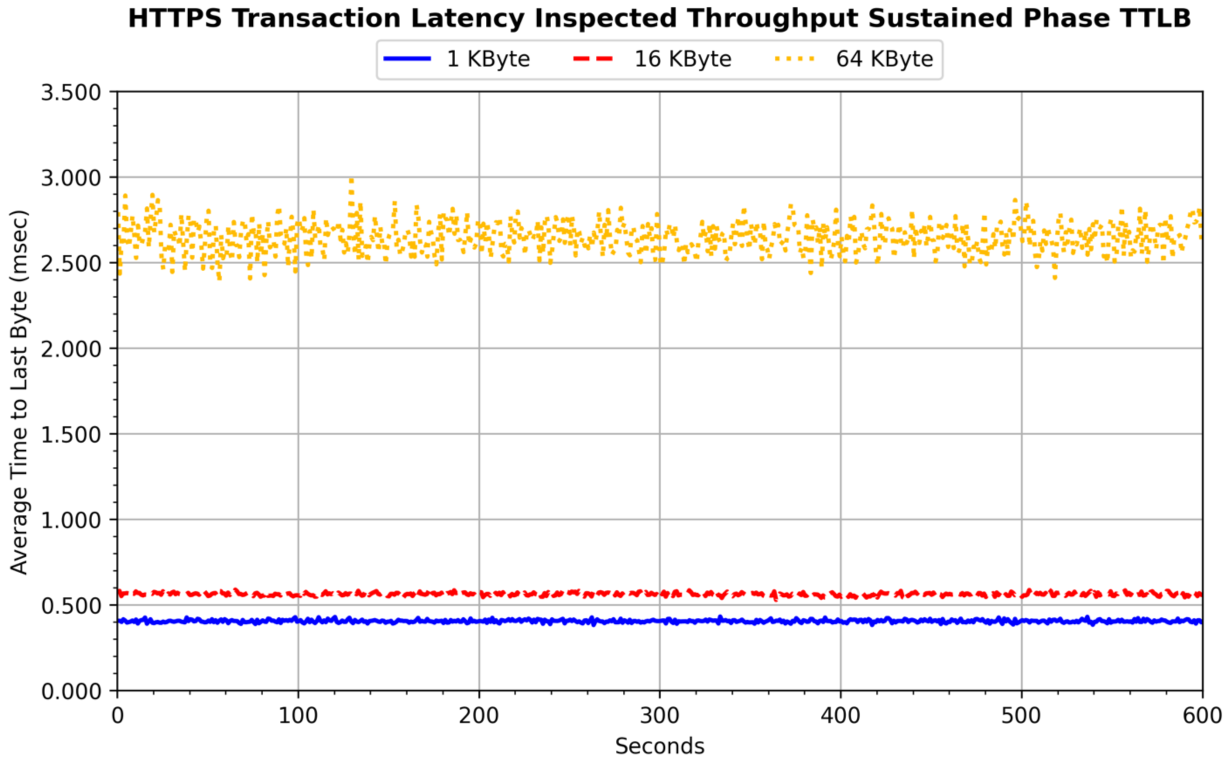
Sustainable inspected throughput of the DUT/SUT for HTTPS transactions varying the HTTPS response object size.



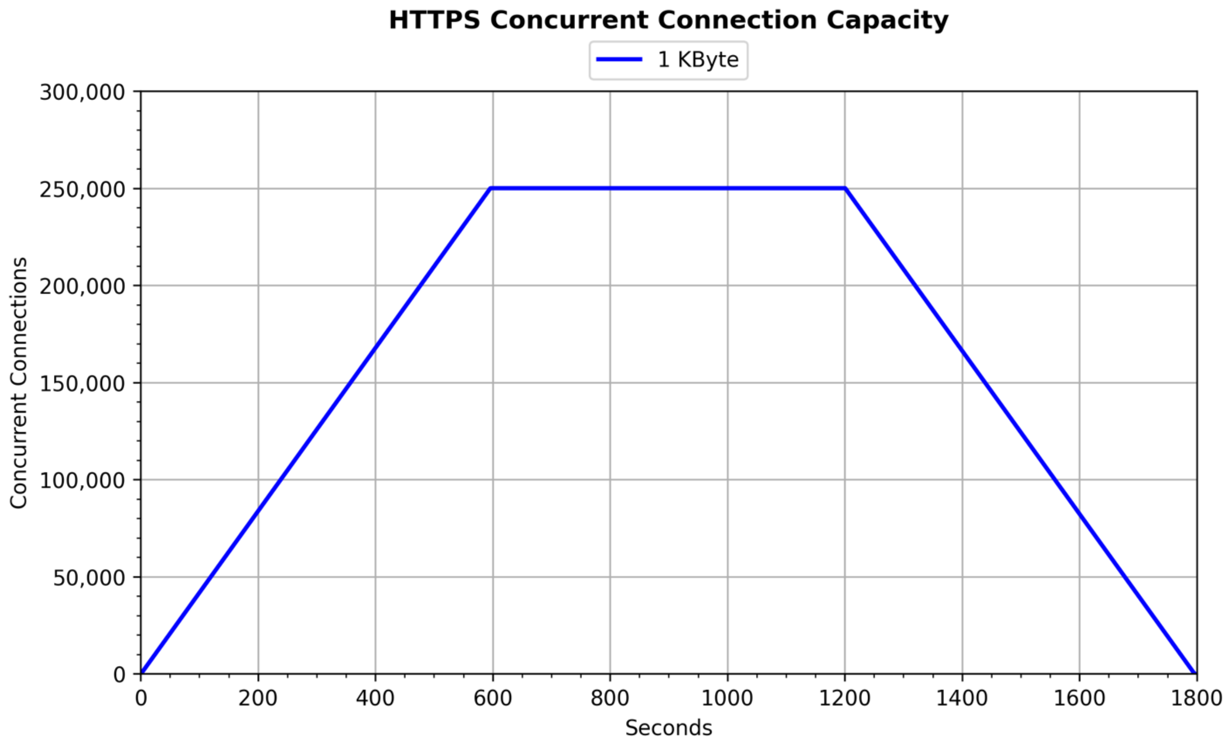


Average HTTPS transaction latency time to first byte under different HTTPS response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.





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).

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	176	4
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)	28.70 (28,696,000)				26.48 (26,485,000)			
	TPS	107,054				124,641			
	CVE	Unique CVEs	Scenarios total	Blocked	Not Blocked	Unique CVEs	Scenarios total	Blocked	Not Blocked
		50	7,060	7,060	0	50	7,060	7,060	0