



University of New Hampshire  
InterOperability  
Laboratory

# NetSecOPEN TEST REPORT

April 2021

MIKE DEICHMAN  
 WATCHGUARD TECHNOLOGIES INC.  
[MIKE.DEICHMAN@WATCHGUARD.COM](mailto:MIKE.DEICHMAN@WATCHGUARD.COM)

DEVICE AND TEST PLAN INFORMATION	
Device Under Test (DUT)	Firebox T40
Test Specification/Suite	Benchmarking Methodology for Network Security Device Performance draft-ietf-bmwg-ngfw-performance-06
UNH-IOL Test Result ID	33331

CONTACT INFORMATION		
Testing Completed by	Chris Brown	<a href="mailto:cbrown@iol.unh.edu">cbrown@iol.unh.edu</a>
Report Created by	Chris Brown	<a href="mailto:cbrown@iol.unh.edu">cbrown@iol.unh.edu</a>
Report Reviewed by	Michayla Newcombe	<a href="mailto:mnewcombe@iol.unh.edu">mnewcombe@iol.unh.edu</a>
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

Throughput performance with NetSecOPEN traffic mix portion of the methodology is currently still under development; therefore, not reported.

Both public and private Common Vulnerabilities and Exposures (CVE) sets were tested against the device under test to confirm that the device exhibited the enabled security functionality. This portion of the methodology is currently still under development; therefore, the results are not officially reported for NetSecOPEN certification.

## REVISION HISTORY

The following table contains a revision history for this report.

REVISION	DATE	AUTHOR	EXPLANATION
1.0	04/15/2021	Chris Brown	Initial version

## DEVICE INFORMATION

COMPONENT	DESCRIPTION
Device Name	Firebox T40
UNH-IOL Device Identification Number	FW-WATCHGRD-0000027764
Device Model	T40
Device Firmware	12.6.4.B635642
Interfaces Tested	Ethernet 1, Ethernet 2, Ethernet 3, Ethernet 4
Interfaces Speed	1G
Controller Name	N/A
Controller Model	N/A
Controller Firmware	N/A
Virtual VNF	N/A
VM Cores Used	N/A
VM RAM Used	N/A
Pinning Information	N/A
Hypervisor Name	N/A
Hypervisor Version	N/A

## DEVICE ENABLED FEATURES

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

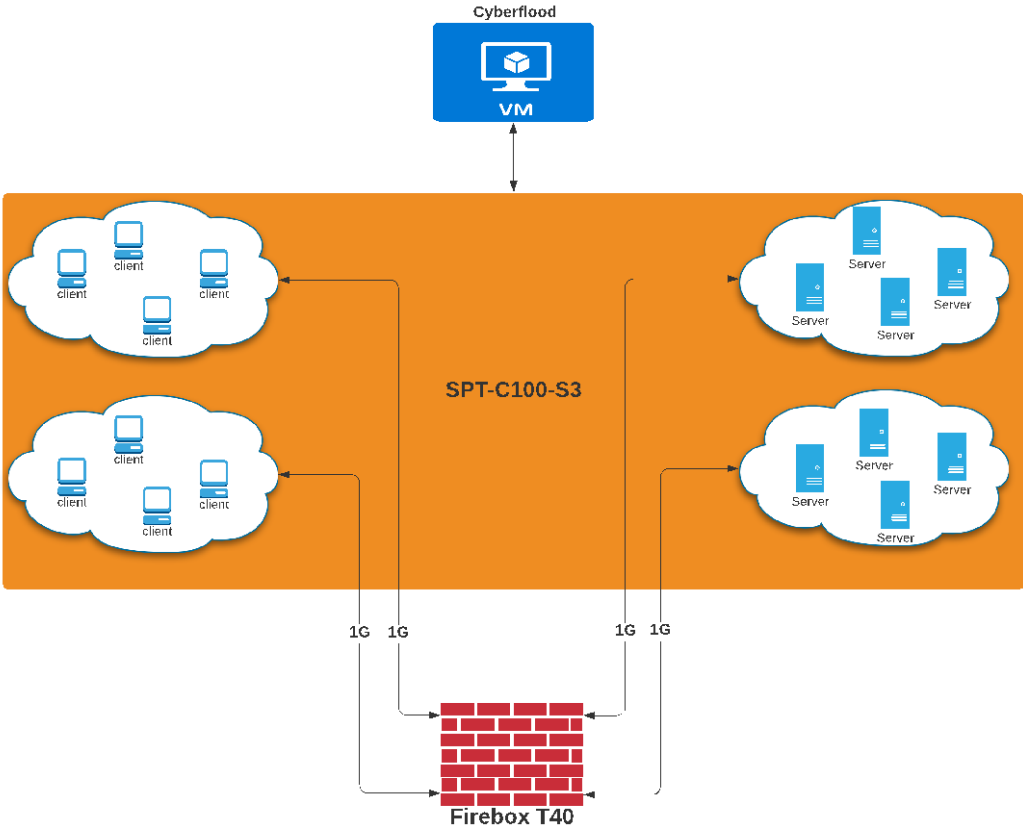
## DEVICE ACL RULES

RULE TYPE	ACTION	# OF RULES
Application Layer	Block	5
Transport Layer	Block	25
IP Layer	Block	25
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	5.18.0309	
Performance Hardware Interface Type	1G	
Performance Application Software Name	Cyberflood	
Performance Application Software Version	21.1.4286	
Efficiency Test Equipment Vendor	Spirent	
Efficiency Hardware Name	SPT-C100-S3	
Efficiency Hardware Firmware	5.18.0309	
Efficiency Hardware Interface Type	1G	
Efficiency Application Software Name	Cyberflood	
Efficiency Application Software Version	21.1.4286	
Client IP Subnet 1	10.10.0.0/21	
Client IP Subnet 2	10.12.0.0/21	
Server IP Subnet 1	10.11.0.0/21	
Server IP Subnet 2	10.13.0.0/21	
Traffic Distribution Ratio	<b>IPv4</b>	<b>IPv6</b>
	100%	0%
Cipher Suite	ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048	

# TESTBED SETUP



## KPI RESULT SUMMARY

### SECTION 7.1

TEST CASE	KPI	TRAFFIC MIX (SSL DISABLED)	TRAFFIC MIX (SSL ENABLED)
Throughput Performance with NetSecOPEN Traffic Mix	Throughput	N/A	N/A
	TPS	N/A	N/A
	TTFB	N/A	N/A
	TTLB	N/A	N/A

### SECTION 7.2

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTP Connections Per Second	CPS	1,149	1,067	979	694	337

### SECTION 7.3

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTP Throughput	TPUT (Kbit/s)	22,561	144,234	236,985	287,482	215,640
	TPS	1,817	1,055	442	135	489



## 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)	2.8	3.3	4.5	3.3	3.2	4.3
	TTFB Minimum (msec)	1.98	1.96	2.01	1.87	1.87	1.95
	TTFB Maximum (msec)	99.07	189.90	83.25	95.43	116.23	231.12
	TTLB Average (msec)	2.6	4.3	9.3	202.8	3.4	7.9
	TTLB Minimum (msec)	1.95	3.11	7.63	201.38	2.48	6.41
	TTLB Maximum (msec)	91.78	204.57	96.66	312.37	203.97	239.68

## SECTION 7.5

TEST CASE	KPI	1K
Concurrent TCP/HTTP Connection Capacity	CC	131,220

## SECTION 7.6

TEST CASE	KPI	1K	2K	4K	16K	64K
TCP/HTTPS Connections Per Second	CPS	101	100	99	93	78
	HR	1K				

## SECTION 7.7

TEST CASE	KPI	1K	16K	64K	256K	MIX
HTTPS Throughput	TPUT (Kbit/s)	10,159	65,978	139,575	196,855	126,651
	TPS	632	471	257	92	284

## SECTION 7.8

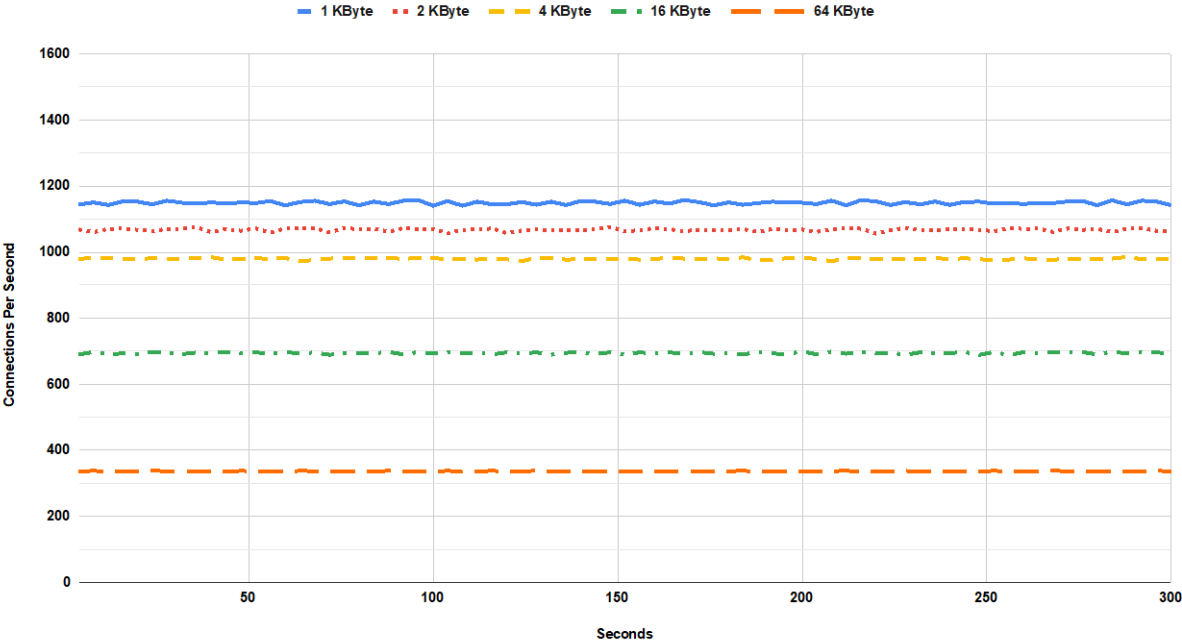
TEST CASE	KPI	CPS 1K	CPS 16K	CPS 64K	TPUT 1K	TPUT 16K	TPUT 64K
TCP/HTTPS Transaction Latency	TTFB Average (msec)	38.3	37.8	39.3	41.4	37.9	39.3
	TTFB Minimum (msec)	33.75	33.82	33.95	34.66	34.09	34.43
	TTFB Maximum (msec)	109.11	106.45	105.05	134.93	87.69	88.29
	TTLB Average (msec)	177.9	180.0	239.4	224.8	22.3	39.1
	TTLB Minimum (msec)	116.71	89.20	137.23	201.86	3.77	9.72
	TTLB Maximum (msec)	231.28	376.80	456.77	443.46	231.72	809.41

## SECTION 7.9

TEST CASE	KPI	1K
Concurrent TCP/HTTPS Connection Capacity	CC	21,600

# GRAPHS

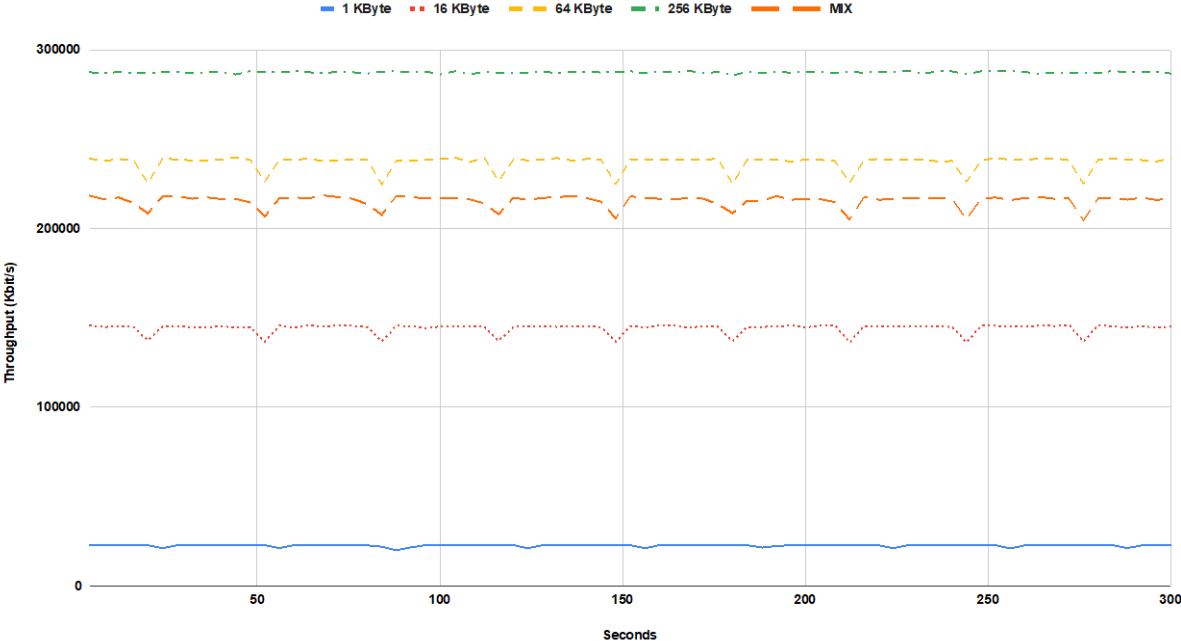
TCP/HTTP Connections Per Second Sustained Phase



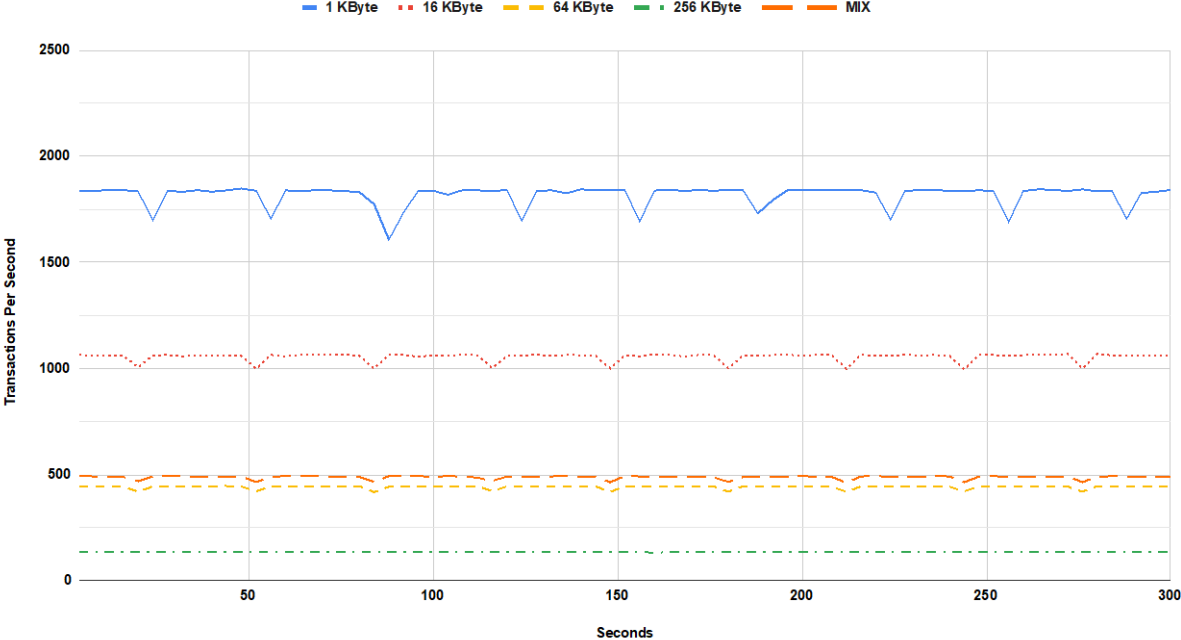
Sustainable TCP/HTTP connection establishment rate supported by the DUT/SUT under different throughput load conditions.



### HTTP Throughput Sustained Phase



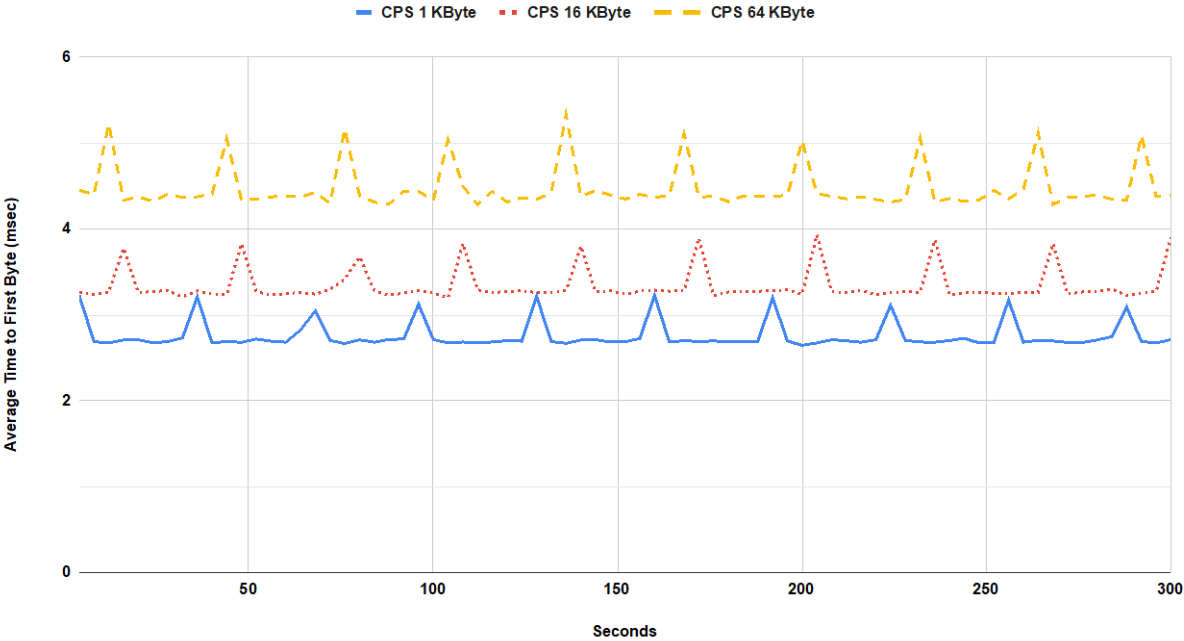
### HTTP Transactions Per Second Sustained Phase



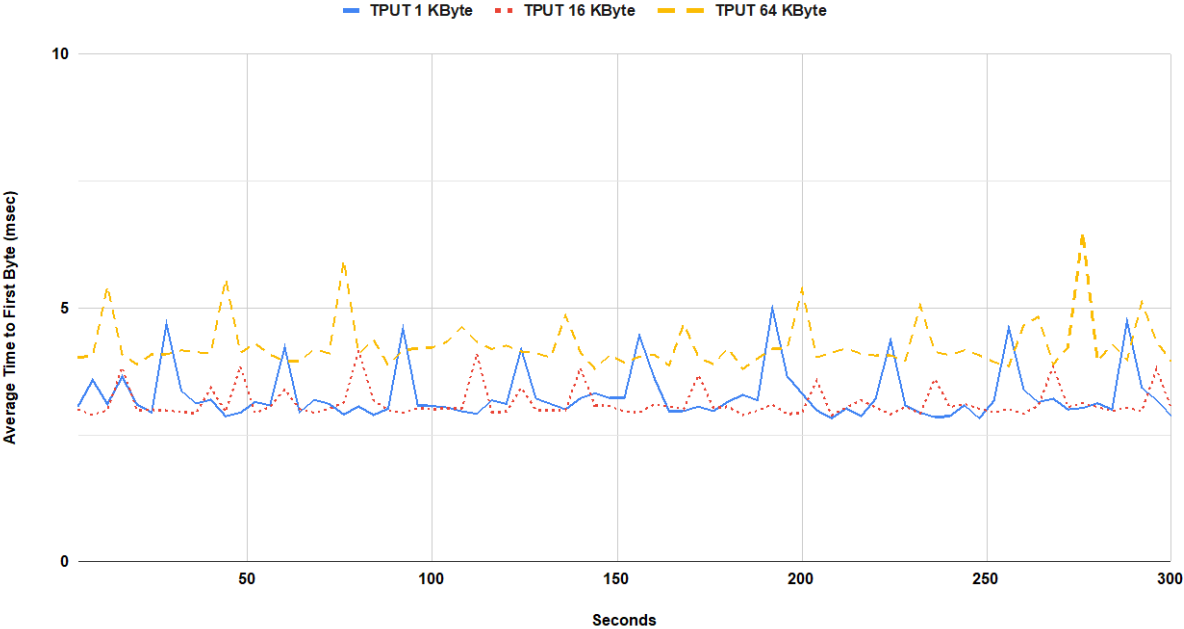
Sustainable throughput for of the DUT/SUT for HTTP transactions varying the HTTP response object size.



### TCP/HTTP Transaction Latency Connections Per Second Sustained Phase



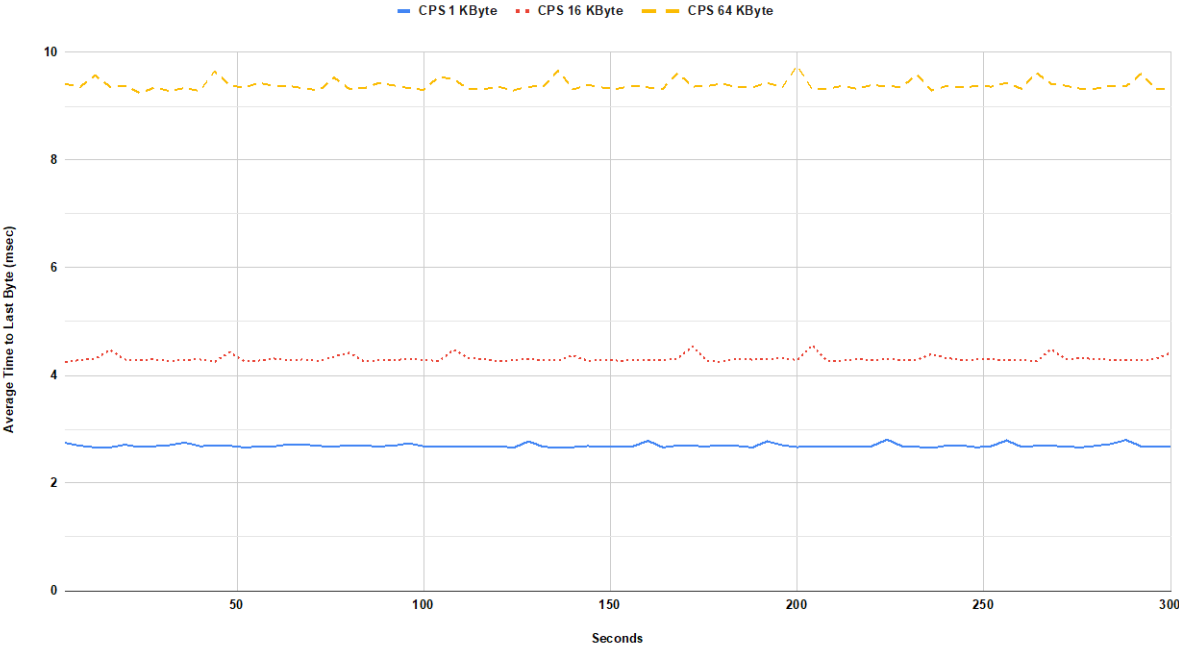
### TCP/HTTP Transaction Latency Throughput Sustained Phase



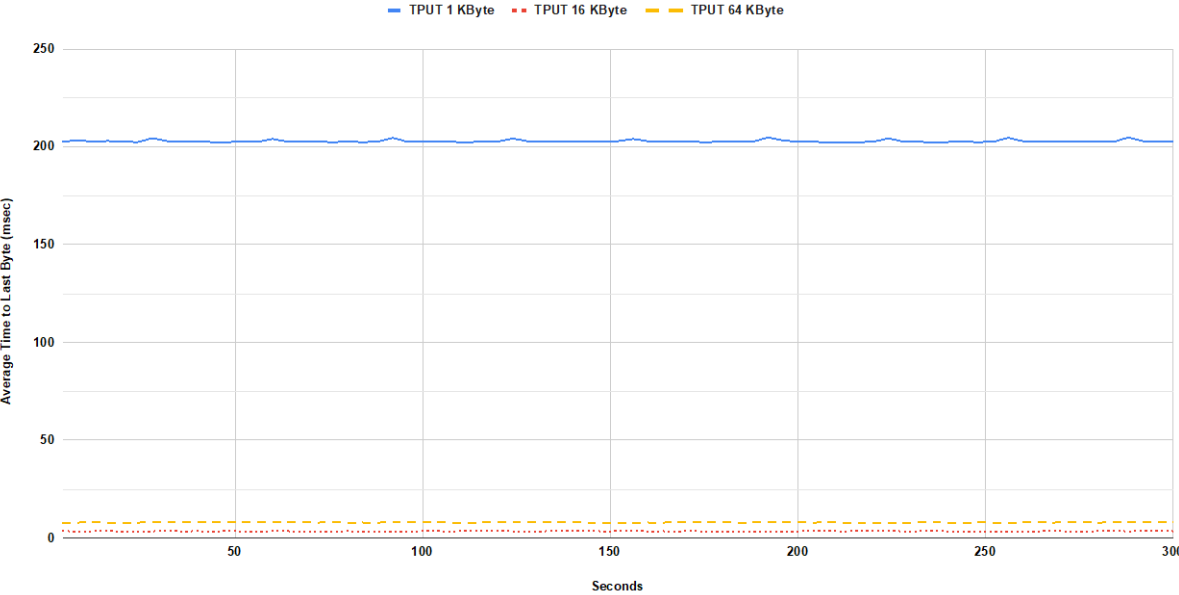
Average HTTP transaction latency time to first byte under different HTTP response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.



### TCP/HTTP Transaction Latency Connections Per Second Sustained Phase



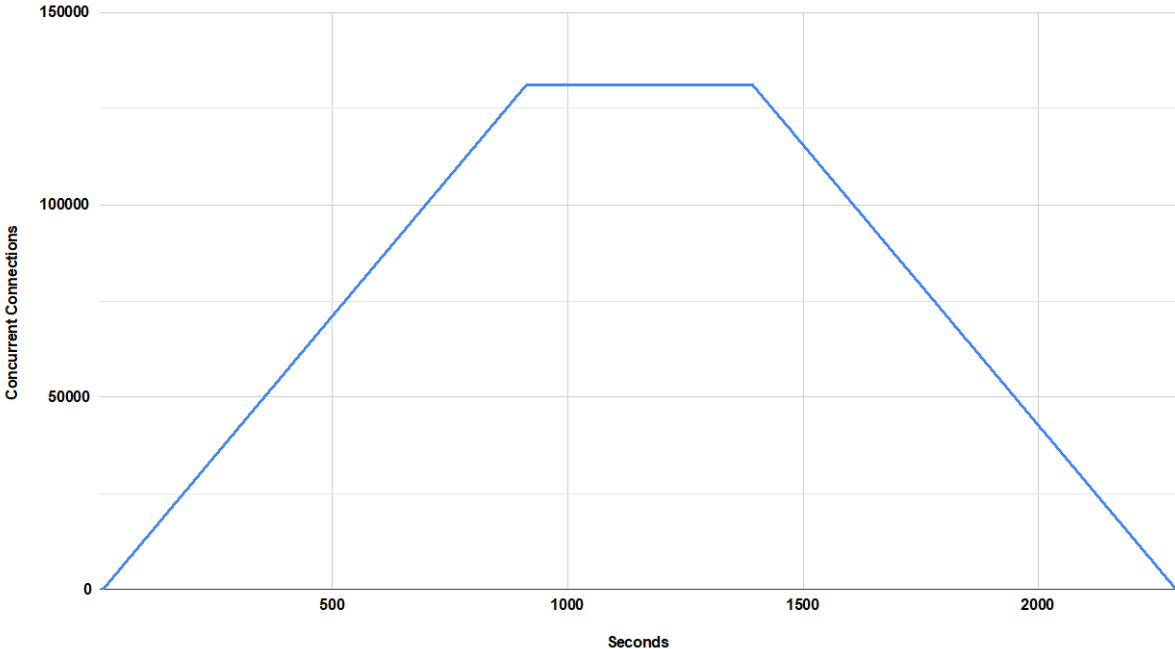
### TCP/HTTP Transaction Latency Throughput Sustained Phase



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

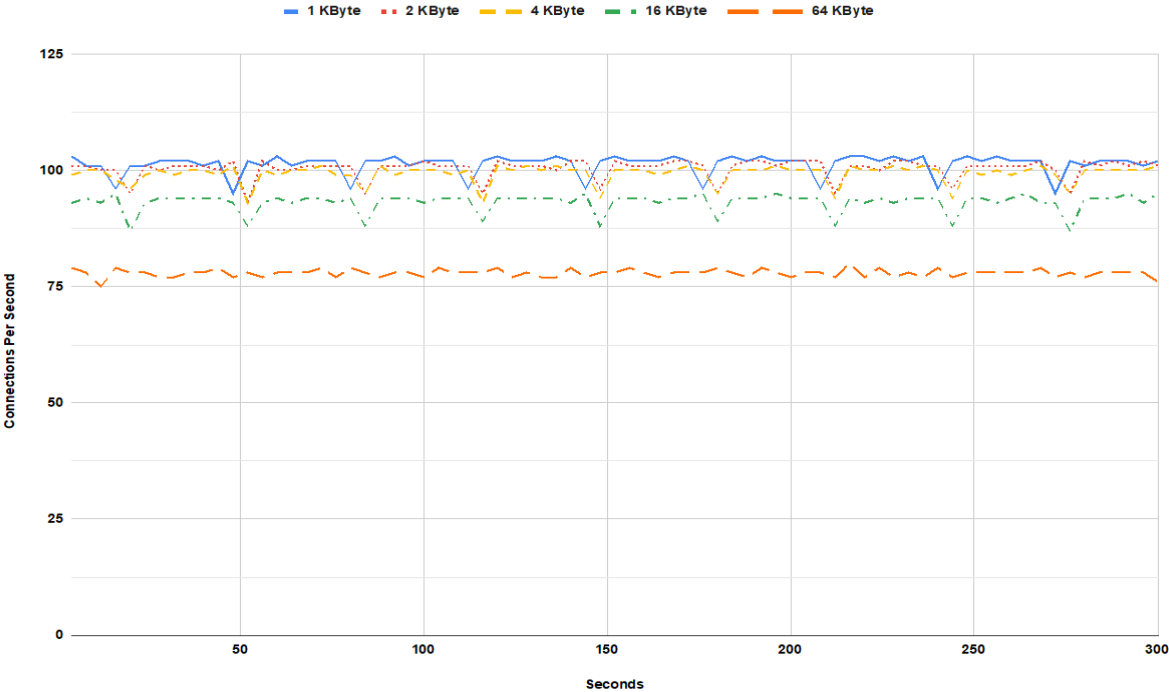


Number of concurrent TCP connections that the DUT/SUT sustains when using HTTP traffic.

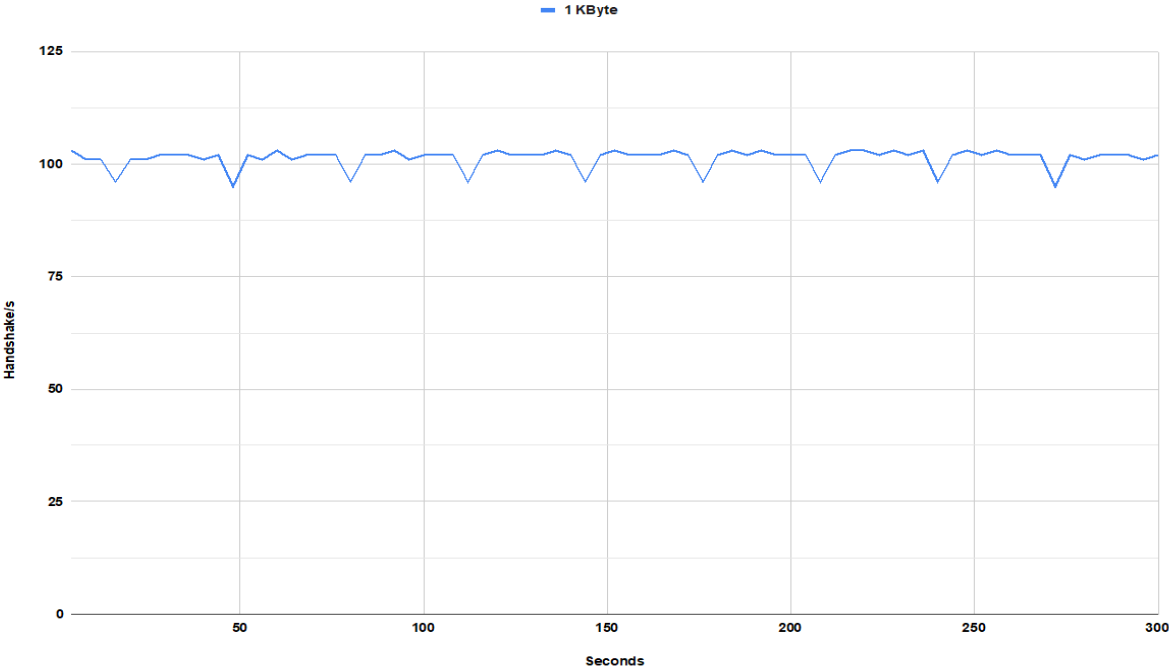




### TCP/HTTPS Connections Per Second Sustained Phase



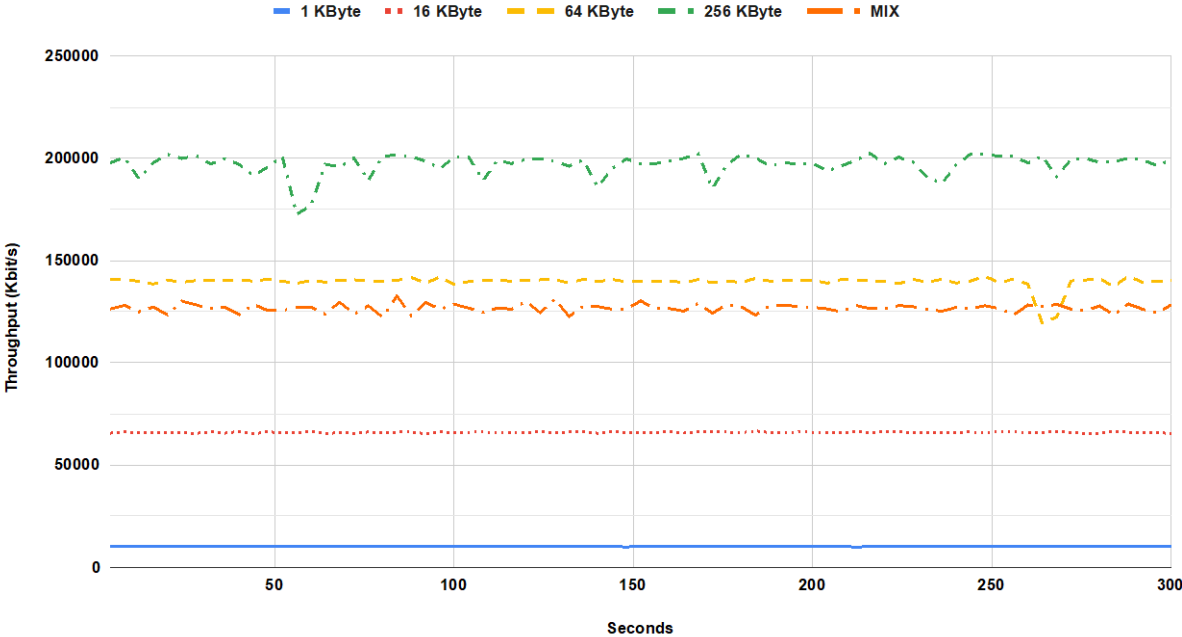
### TCP/HTTPS TLS Handshake Rate Sustained Phase



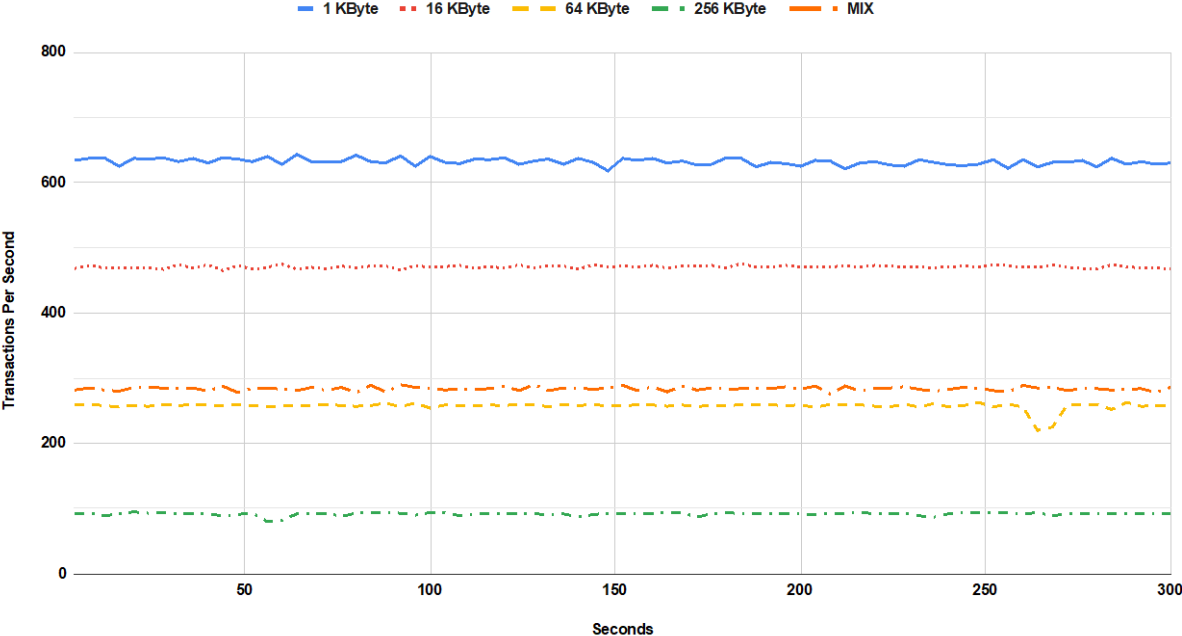
Sustainable SSL/TLS session establishment rate supported by the DUT/SUT under different throughput load conditions.



### HTTPS Throughput Sustained Phase



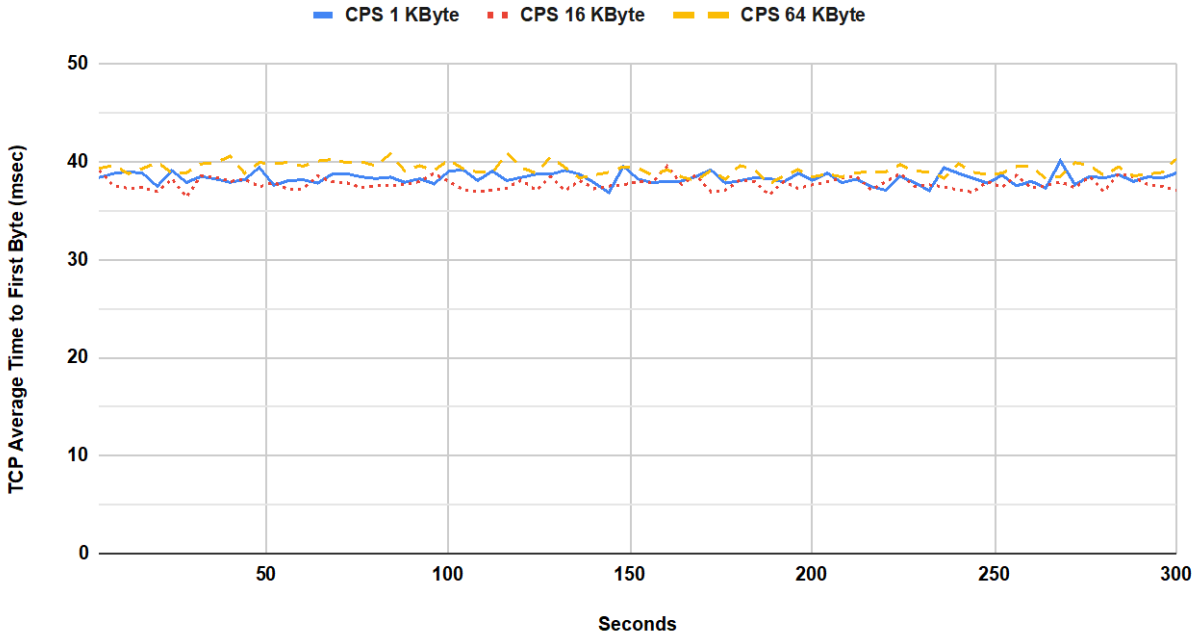
### HTTPS Transactions Per Second Sustained Phase



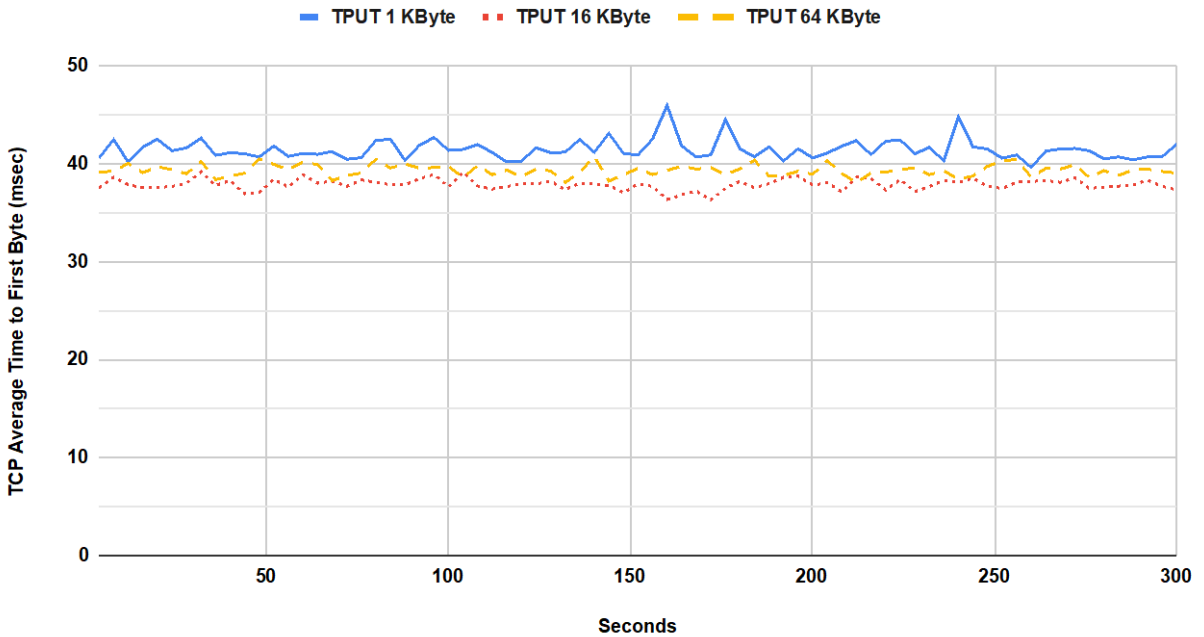
Sustainable throughput for of the DUT/SUT for HTTPS transactions varying the HTTPS response object size.



### TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase

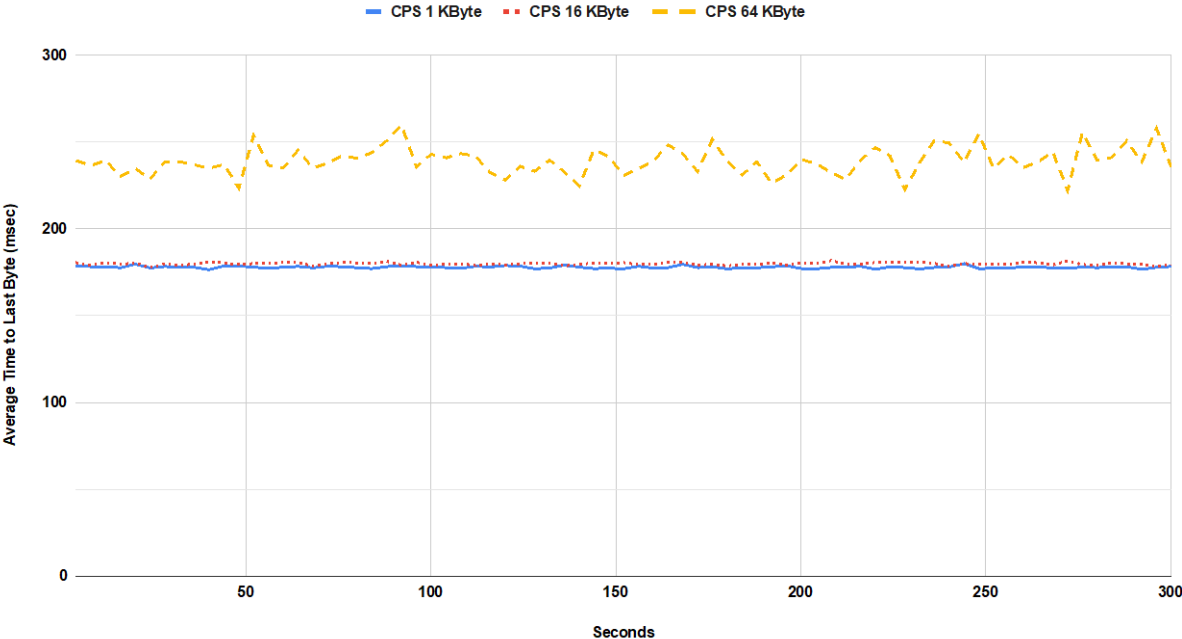


### TCP/HTTPS Transaction Latency Throughput Sustained Phase

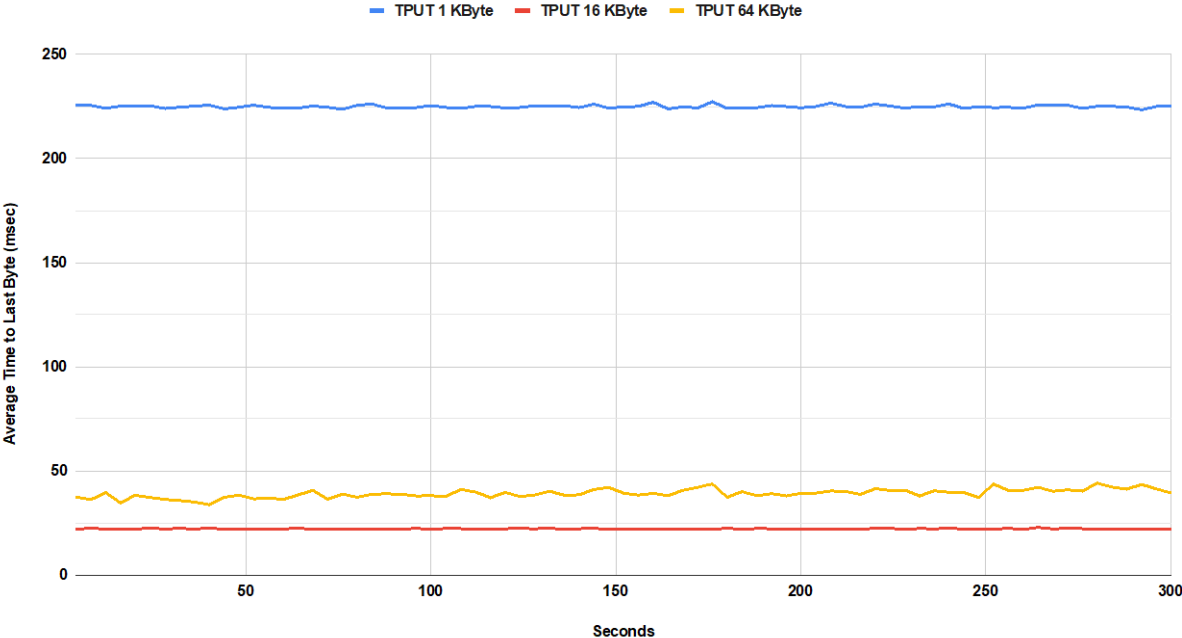


Average HTTPS transaction latency time to first byte under different HTTPS response object sizes. First scenario with a single transaction and the second scenario is with multiple transactions within a single TCP connection.

### TCP/HTTPS Transaction Latency Connections Per Second Sustained Phase



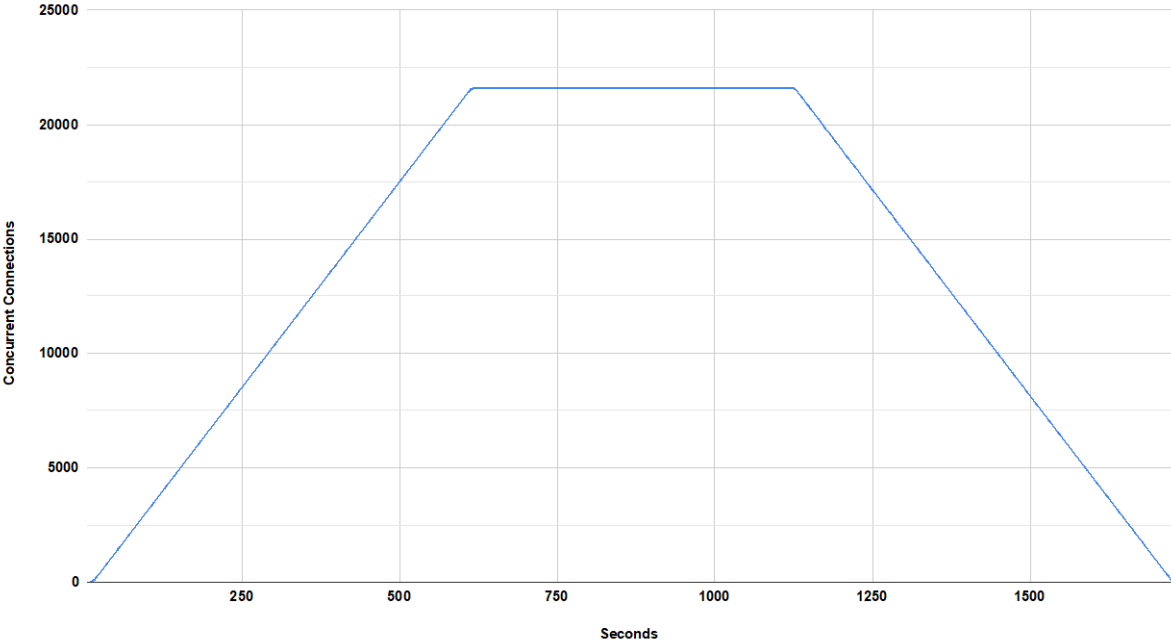
### TCP/HTTPS Transaction Latency Throughput Sustained Phase



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
<b>CPS</b>	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. The TCP connection must be initiated via a TCP 3-way handshake (SYN, SYN/ACK, ACK). Then the TCP session data is sent. The TCP session <b>MUST</b> be closed via either a TCP 3 way close (FIN, FIN/ACK, ACK), or a TCP 4 way close (FIN, ACK, FIN, ACK), and not by a RST.
<b>HR</b>	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.
<b>TPUT</b>	Throughput	The number of bits per second of allowed traffic a DUT/SUT can be observed to transmit to the correct destination interface(s) in response to a specified offered load (defined in <a href="#">RFC2647</a> ). The throughput benchmarking tests <b>SHOULD</b> measure the average throughput value.
<b>TPS</b>	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 HTTP(S) transaction, it must have a valid status code, and the appropriate FIN, FIN/ACK sequence must have been completed.
<b>TTFB</b>	Time to First Byte	TTFB is the elapsed time between the start of sending the TCP SYN packet from the client and the client receiving the first packet of application data from the server or DUT/SUT. The benchmarking tests HTTP Transaction Latency and HTTPS Transaction Latency measure the minimum, average and maximum TTFB. The value <b>SHOULD</b> be expressed in millisecond.
<b>TTLB</b>	Time to Last Byte	URL Response time / TTLB is the elapsed time between the start of sending the TCP SYN packet from the client and the client receiving the last packet of application data from the server or DUT/SUT. The benchmarking tests HTTP Transaction Latency and HTTPS Transaction Latency measure the minimum,

		average and maximum TTLB. The value SHOULD be expressed in millisecond.
<b>CC</b>	Concurrent TCP Connections	The aggregate number of simultaneous connections between hosts across the DUT/SUT, or between hosts and the DUT/SUT (defined in <a href="#">RFC2647</a> ).
<b>N/A</b>	Not Applicable	This test does not apply to the device type or is not applicable to the testing program selected.

## APPENDIX 2: CVE DETECTION RATES

As stated previously, we performed the CVE check to verify the security functionality of the DUT during performance test. Two vulnerability sets were used, one Public and one Private (The private set was not known to the DUT vendor in order to ensure the test was not being gamed). The public set contained approximately 435 CVEs and the private set contained approximately 30 CVEs.

As a preview to the security effectiveness test methodology under development, following are the respective private and public block rates used to verify security functionalities/modules are engaged.

The block rates for this test are:

PREVENT SCENARIO	SCENARIOS TOTAL	BLOCKED	NOT BLOCKED
Public CVE	435	430	5
Private CVE	33	31	2