



NetSecOPEN Certification

Network Security Product Performance Testing

WatchGuard Firebox T40

Testing Information

Vendor: WatchGuard Technologies INC.

Product name and Model: Firebox T40

Product version: 12.6.4 (Build 635642)

Test Lab: University of New Hampshire Interoperability Lab

Test equipment: Spirent CyberFlood C100-S3

Test equipment version: Firmware: 5.18.0309 , Software: 21.1.4286

Test Date and Location: April 16, 2021 Durham, NH

Tested based on draft-ietf-bmwg-ngfw-performance-06 (<https://tools.ietf.org/html/draft-ietf-bmwg-ngfw-performance-06>)

Executive Summary

Introduction

The goal of NetSecOPEN is to provide performance testing standards developed by the membership, implemented on approved test tools and used by accredited test labs. These goals are intended to promote transparency and reproducibility. To achieve these goals the accredited labs freely provide access to their test reports, Device under Test (DUT) vendors provide the configuration of the DUT as it was tested and the test tool vendors provide the default configuration, while the lab documents changes to the test tool in the report.

All of these are provided at no charge to interested parties. Anyone interested in having access to the configuration files please e-mail the NetSecOPEN Certification Body at netsecopen-cert-body@netsecopen.org.

Summary of Findings

The NetSecOPEN Certification Body has reviewed the test report of the Firebox T40 provided by University of New Hampshire InterOperability Lab. These results have been found to meet the NetSecOPEN certification requirements. Detailed results are provided below.

NetSecOPEN Certification is awarded to WatchGuard Technology's Firebox T40 (version 12.6.4, Build 635642).

Note: this certification is product and version specific.

Results Summary

The tables 1 & 2 below highlight the measured values for the Key Performance indicators (KPIs). The values for individual object sizes and test scenarios are described in the section “Detailed Test Results”

HTTP Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	1,149 CPS @ 1 KByte and 337 CPS @ 64 KByte object sizes
Throughput	287.5 Mbit/s @ 256 KByte and 22.6 Mbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	1,817 TPS @ 1 KByte and 135 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	3.3 ms average TTFB @ 1 KByte and 4.3 ms average TTFB @ 64 KByte object sizes ¹ 2.8 ms average TTFB @ 1 KByte and 4.5 ms average TTFB @ 64 KByte object sizes ²
Time to Last Byte (TTLB)	202.8 ms average TTLB @ 1 KByte and 7.9 ms average TTLB @ 64 KByte object sizes ¹ 2.6 ms average TTLB @ 1 KByte and 9.3 ms average TTLB @ 64 KByte object sizes ²
Concurrent connection	131,220 average concurrent connection

Table 1: Results summary for HTTP tests

HTTPS Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	101 CPS @ 1 KByte and 78 CPS @ 64 KByte object sizes
Throughput	196.9 Mbit/s @ 256 KByte and 10.2 Mbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	632 TPS @ 1 KByte and 92 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	41.4 ms average TTFB @ 1 KByte and 39.3 ms average TTFB @ 64 KByte object sizes ¹ 38.3 ms average TTFB @ 1 KByte and 39.3 ms average TTFB @ 64 KByte object sizes ²
Time to Last Byte (TTLB)	224.8 ms average TTLB @ 1 KByte and 39.1 ms average TTLB @ 64 KByte object sizes ¹ 177.9 ms average TTLB @ 1 KByte and 239.4 ms average TTLB @ 64 KByte object sizes ²
Concurrent connection	21,600 average concurrent connection

Table 2: Results summary for HTTPS tests

¹ Tested with 50% of max. throughput that the Firebox T40 supported.

² Tested with 50% of max. CPS that the Firebox T40 supported.

Test setup and configurations

All the tests were performed with test setup (option 2) defined in the draft in [section 4.1](#). four 1GbE interfaces of the Firebox T40 were directly connected with the test equipment.

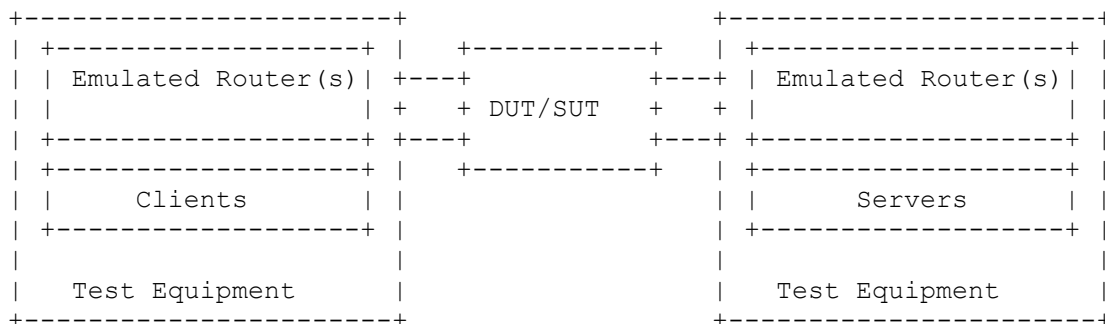


Figure 1: Testbed Setup

The table below shows the recommended and optional Next Generation Firewall (NGFW) features described in the draft that were enabled/disabled on the security device.

Features		Security device Status
SSL Inspection	Recommended	Enabled
IDS/IPS	Recommended	Enabled
Antivirus	Recommended	Enabled
Anti Spyware	Recommended	Enabled
Anti Botnet	Recommended	Enabled
Logging and Reporting	Recommended	Enabled
Application Identification	Recommended	Enabled
Web Filtering	Optional	Disabled
DLP	Optional	Disabled
DDoS	Optional	Disabled
Certificate Validation	Optional	Disabled

Table 3: NGFW security features

As defined in the draft ([section 4.2](#) table 3, DUT classification “XS”) 69 ACL rules were configured on the Firebox T40.

Before the performance tests were started, the Common Vulnerabilities and Exposures (CVE) tests were performed to ensure the security feature “Detection of Common Vulnerabilities and Exposures (CVE)” was enabled on the Firebox T40 security device. The Firebox T40 detected and blocked attack attempts during this test, indicating that inspection/blocking capability was enabled and functioning.

All tests were performed with IPv4 traffic only. The ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048 cipher suite was used for all the HTTPS performance tests. The latency values represent in the **Error! Reference source not found.** and **Error! Reference source not found.** measured with 50% of the maximum throughput supported by the Firebox T40.

Detailed Test Results

TCP/HTTP Connections Per Second

Object Size [KByte]	Avg. TCP/HTTP Connections Per Second
1	1,149
2	1,067
4	979
16	694
64	337

Table 4: TCP/HTTP Connections per Second

HTTP Throughput and Transactions per Second

Object Size [KByte]	Avg. HTTP Throughput [Mbit/s]	Avg. HTTP Transaction Per Second
1	22.56	1,817
16	144.23	1,055
64	236.98	442
256	287.48	135
Mixed objects	215.64	489

Table 5: HTTP Throughput

TCP/HTTP Transaction Latency

The test was performed with two traffic load profile as defined in the draft. Table 6 below describes the latency results measured with 50% of the maximum connection per second supported by Firebox T40.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	avg	Max
1	1.98	2.8	99.07	1.95	2.6	91.78
16	1.96	3.3	189.90	3.11	4.3	204.57
64	2.01	4.5	83.25	7.63	9.3	96.66

Table 6: TCP/HTTP TTFB and TTLB @ 50% of the maximum connection per second

Table 7 below describes latency results measured with 50% of the maximum throughput supported by Firebox T40.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	avg	Max
1	1.87	3.3	95.43	201.38	202.8	312.37
16	1.87	3.2	116.23	2.48	3.4	203.97
64	1.95	4.3	231.12	6.41	7.9	239.68

Table 7: TCP/HTTP TTFB and TTLB @ 50% of the maximum Throughput

Figures 2-4 illustrate the distribution of maximum latency (TTFB and TTLB) values measured in approximately 76 measurement samples.

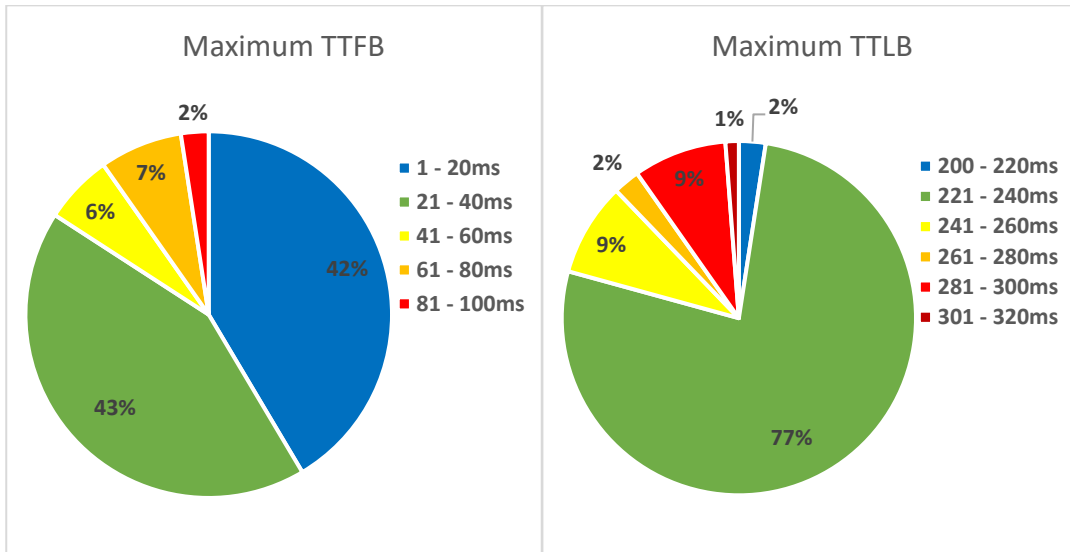


Figure 2: Latency distribution measured with 1KByte object size in Throughput test scenario

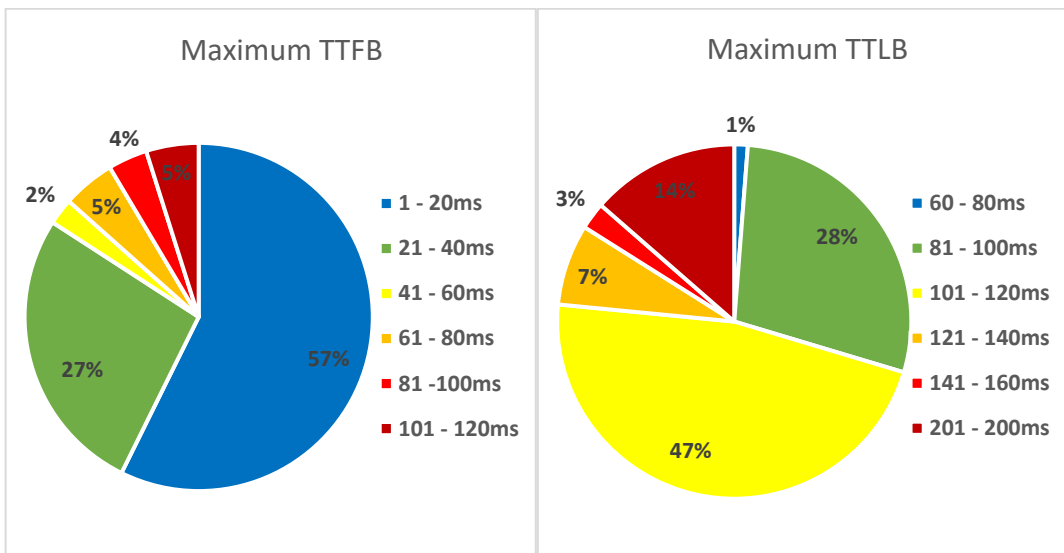


Figure 3: Latency distribution measured with 16KByte object size in Throughput test scenario

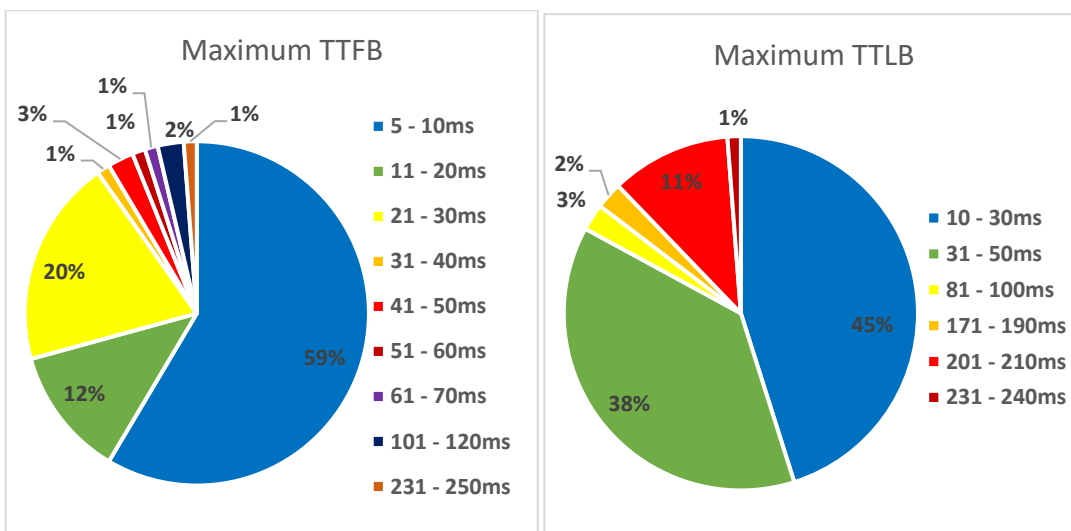


Figure 4: Latency distribution measured with 64KByte object size in Throughput test scenario

Concurrent TCP/HTTP Connection Capacity

The Firebox T40 supported 131,220 concurrent TCP/HTTP connection in average. 1 KByte object size was used as HTTP GET request for each established TCP connection, which resulted an average throughput of 10.7 Mbit/s.

TCP/HTTPS Connections per second

Object Size [KByte]	Avg. TCP/HTTPS Connections Per Second
1	101
2	100
4	99
16	93
64	78

Table 8: TCP/HTTPS Connections per Second

HTTPS Throughput

Object Size [KByte]	Avg. HTTPS Throughput [Mbit/s]	Avg. HTTPS Transaction Per Second
1	10.16	632
16	65.98	471
64	139.57	257
256	196.86	92
Mixed objects	126.65	284

Table 9: HTTPS Throughput

HTTPS Transaction Latency

The test was performed with two traffic load profile as defined in the draft. Table 10 below describes the latency results measured with 50% of the maximum connection per second supported by FireBox T40.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	avg	Max
1	33.75	38.3	109.11	116.71	177.9	231.28
16	33.82	37.8	106.45	89.2	180	376.8
64	33.95	39.3	105.05	137.23	239.4	456.77

Table 10: TCP/HTTPS TTFB and TTLB @ 50% of the maximum connection per second

Table 11 below describes latency results measured with 50% of the maximum throughput supported by FireBox T40.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	avg	Max
1	34.66	41.4	134.93	201.86	224.8	443.46
16	34.09	37.9	87.69	3.77	22.3	231.72
64	34.43	39.3	88.29	9.72	39.1	809.41

Table11: TCP/HTTP TTFB and TTLB @ 50% of the maximum Throughput

Figures 5 -7 illustrate the distribution of maximum latency (TTFB and TTLB) values measured in approximately 76 measurement samples.

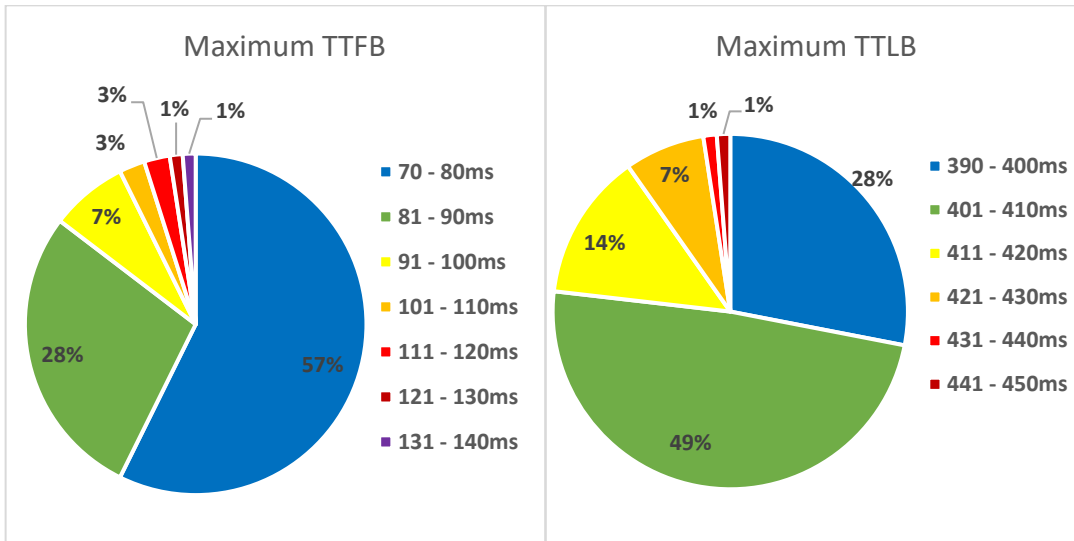


Figure 5: Latency distribution measured with 1KByte object size in Throughput test scenario

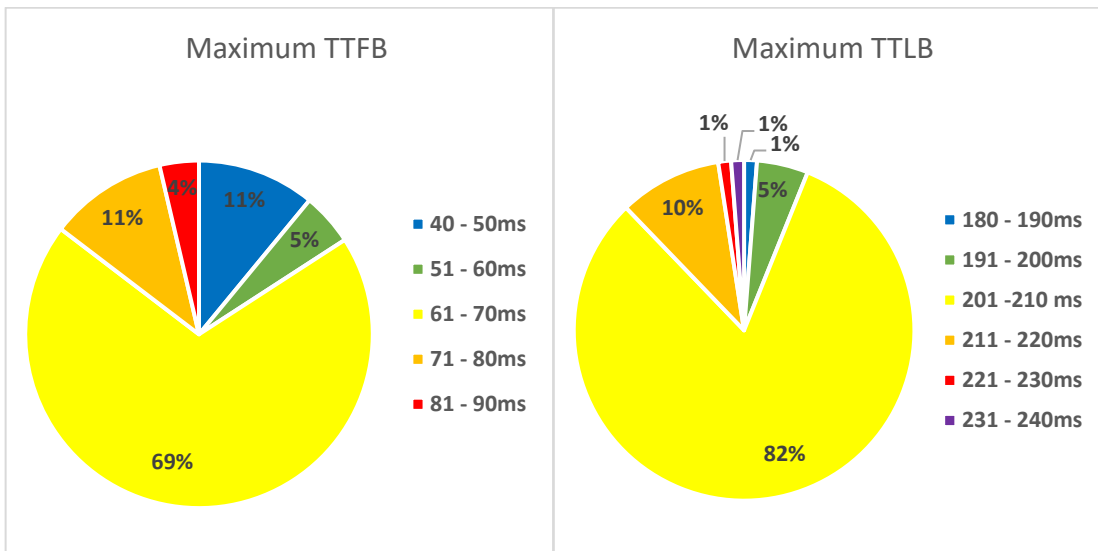


Figure 6: Latency distribution measured with 16KByte object size in Throughput test scenario

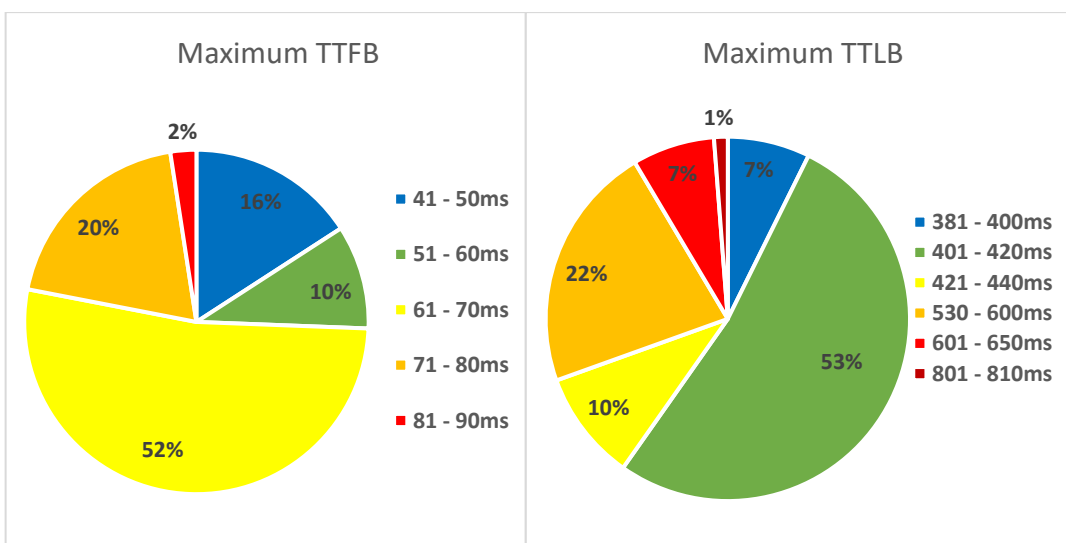


Figure 7: Latency distribution measured with 64KByte object size in Throughput test scenario



Concurrent TCP/HTTPS Connection Capacity

The WatchGuard's Firebox T40 supported 21,600 concurrent TCP/HTTPS connection in average. 1 KByte object size was used as HTTPS GET request for each established TCP connection, which resulted an average throughput of 2.3 Mbit/s.