NetSecOPEN

NetSecOPEN Certification
Network Security Product Performance Testing
Cisco Systems Firepower Threat Defense 4120

Testing Information

Vendor: Cisco Systems

Product name and Model: Firepower Threat Defense 4120

Product version: 6.4.0.4

Performance Test Equipment

Test Lab: University of New Hampshire InterOperability Lab

Test equipment: Spirent Cyberflood C100-S3

Test equipment version: 5.03.0381

Security Effectiveness Test Equipment

Test Equipment: Ixia PerfectStorm One

Test equipment version: 9.00.1900.17

Test Date and Location: January 21, 2020 Durham, NH

Tested based on draft-ietf-bmwg-ngfw-performance-02 (https://tools.ietf.org/html/draft-ietf-bmwg-ngfw-performance-02)

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. All of 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 Firepower 4120 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 Cisco System's Firepower 4120 (6.4.0.4).

Note: this certification is product and version specific.

Test setup and configurations

All the performance tests were conducted with test setup (option 2) defined in the draft in section 4.1. Six 10Gb interfaces of the Firepower 4120 were directly connected with the test equipment.

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[1]
Anti Spyware	Recommended	Enabled[1]
Anti Botnet	Recommended	Enabled[1]
Logging and Reporting	Recommended	Enabled
Application Identification	Recommended	Enabled
Web Filtering	Optional	Disabled
DLP	Optional	Disabled
DDoS	Optional	Disabled
Certificate Validation	Optional	Disabled

Table 1: NGFW security features   [1]These features were on by default. No configuration was done.

 As defined in the draft (section 4.2 table 1, DUT classification "L") 564 ACL rules were configured on Firepower 4120.

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 Cisco Systems security device. Cisco Systems Firepower 4120 successfully 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. ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048 was used as cipher suite for all of the HTTPS performance tests. The latency values represent in the Table 2 and Table 3 measured with 50% of the maximum throughput supported by the Firepower 4120.

Test Results

HTTP Traffic Performance

Object Size [KByte]	Avg. CPS	Avg. TP [Gbit/s]	Avg. TPS	Avg. CC	TTFB [ms]			TTLB [ms]		
					Min	Avg.	Max.	Min	Avg.	Max.
1	45,850	0.9	79,249	14,965,200	0.5	0.9	50.1	<0.0009	0.5	49
2	29,667	NA	NA	NA	NA	NA	NA	NA	NA	NA
4	21,427	NA	NA	NA	NA	NA	NA	NA	NA	NA
16	10,510	2.7	20,079	NA	0.5	1.6	58.1	<0.0009	1.6	62
32	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
64	7,595	6.8	12,720	NA	0.5	1.6	58.4	<0.0009	2.5	80
128	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
256	NA	11	5,146	NA	NA	NA	NA	NA	NA	NA
Mixed	NA	6	13,594	NA	NA	NA	NA	NA	NA	NA

Table 2: TCP/HTTP Traffic Performance
CPS: Connection Per Second, TP: Throughput, TPS: Transactions Per Second, CC: Concurrent Connections, TTFB: Time To First Byte, TTLB: Time To Last Byte, NA: Not Applicable or Not tested

HTTPS Traffic Performance

Object Size [KByte]	Avg. CPS	Avg. TP [Gbit/s]	Avg. TPS	Avg. CC	TTFB [ms]			TTLB [ms]		
					Min	Avg.	Max.	Min	Avg.	Max.
1	6,544	0.4	31,583	145,440	1.9	3.2	59.3	<0.0009	0.9	52
2	6,001	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
4	5,590	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
16	4,813	2.3	15,949	*NA*	1.9	3.9	61.8	1	2.5	56
32	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
64	3,606	5.8	10,620	*NA*	1.9	4.3	65.5	2	3.9	68
128	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
256	*NA*	6.7	3,071	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*
Mixed	*NA*	5.3	11,765	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*	*NA*

Table 3: TCP/HTTPS Traffic Performance
CPS: Connection Per Second, TP: Throughput, TPS: Transactions Per Second, CC: Concurrent Connections, TTFB: Time To First Byte, TTLB: Time To Last Byte, NA: Not Applicable or Not tested

TCP/HTTP Connections Per Second

Object Size [KByte]	Avg. TCP/HTTP Connections Per Second
1	45,850
2	29,667
4	21,427
16	10,510
64	7,595

Table 4: TCP/HTTP Connections per Second

HTTP Throughput

Object Size [KByte]	Avg. HTTP Throughput [Gbit/s]	Avg. HTTP Transaction Per Second
1	0.9	79,249
16	2.7	20,079
64	6.8	12,720
256	11	5,146
Mixed objects	6	13,594

Table 5: HTTP Throughput

TCP/HTTP Transaction Latency

The test was performed with two traffic load profiles as defined in the draft. Table 6 below describes the latency results measured with 50% of the maximum connection per second supported by the Firepower 4120.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	avg	Max
1	0.5	0.9	51.8	<0.0009	0.6	50
16	0.5	1.2	52.1	1	2.3	53
64	0.5	1.1	51.6	1	3.6	58

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 the Firepower 4120.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	avg	Max
1	0.5	0.9	50.1	<0.0009	0.5	49
16	0.5	1.6	58.1	<0.0009	1.6	62
64	0.5	1.6	58.4	<0.0009	2.5	80

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

Figures 1-3 illustrate the distribution of maximum latency (TTFB and TTLB) values measured in approximately 75 measurement samples.
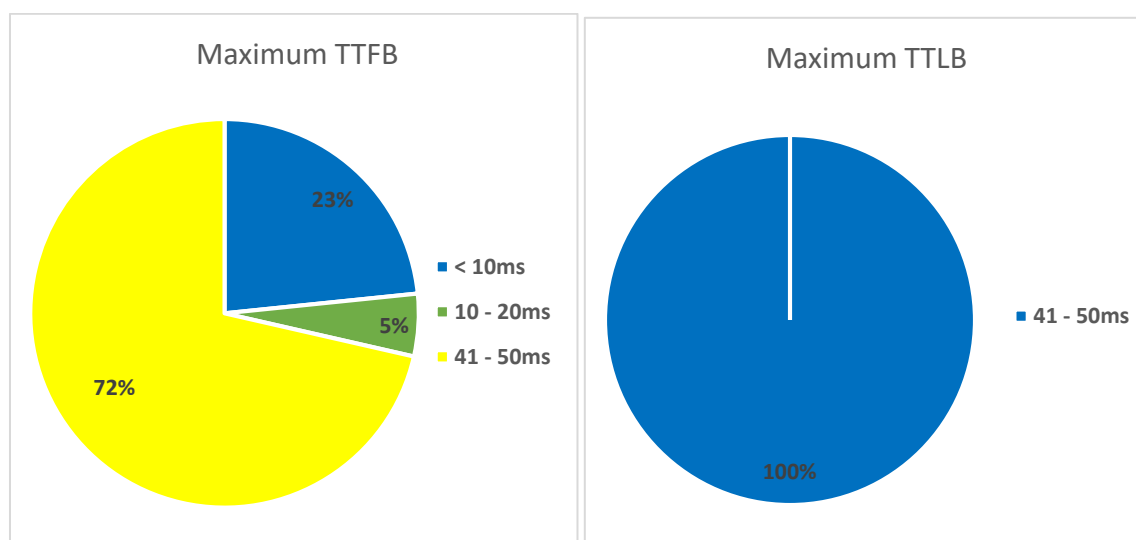

Figure 1:Latency distribution measured with 1KByte object size in Throughput test scenario
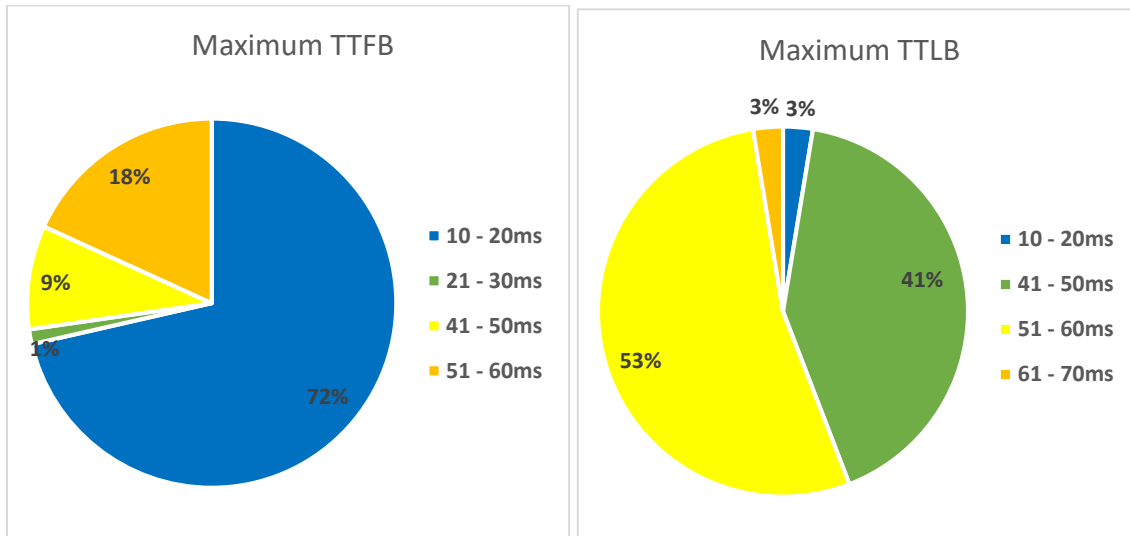
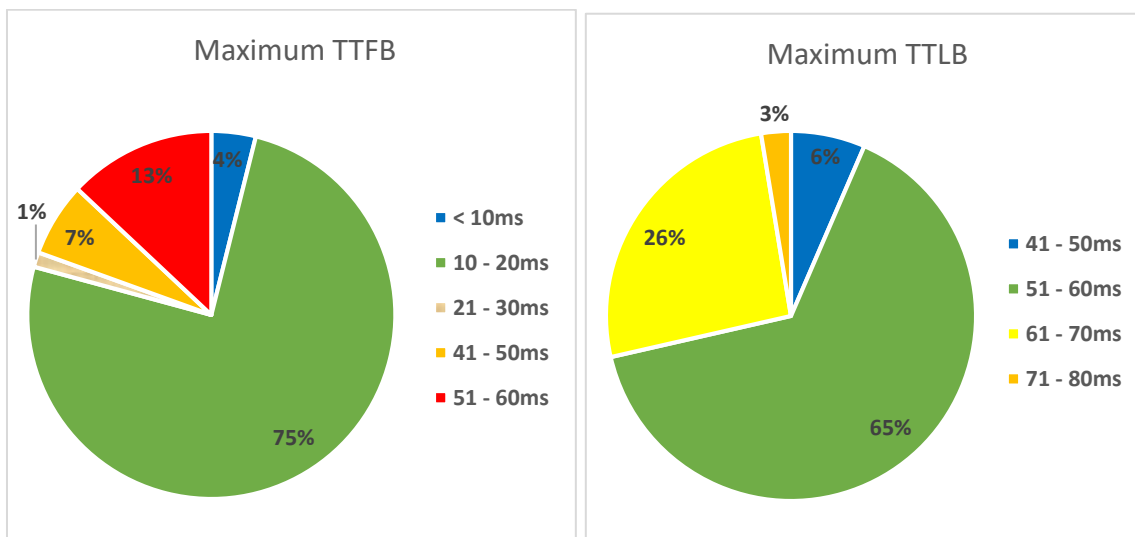*Figure 2: Latency distribution measured with 16KByte object size in Throughput test scenario*

Figure 3:Latency distribution measured with 64KByte object size in Throughput test scenario

Concurrent TCP/HTTP Connection Capacity

The Cisco Systems Firepower 4120 supported 14,965,200 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 912Mbit/s.

TCP/HTTPS Connections per second

Object Size [KByte]	Avg. TCP/HTTPS Connections Per Second
1	6,544
2	6,001
4	5,590
16	4,813
64	3,606

Table 8: TCP/HTTPS Connections per Second

HTTPS Throughput

Object Size [KByte]	Avg. HTTPS Throughput [Gbit/s]	Avg. HTTPS Transaction Per Second
1	0.4	31,583
16	2.3	15,949
64	5.8	10,620
256	6.7	3,071
Mixed objects	5.3	11,765

Table 9: HTTPS Throughput

HTTPS Transaction Latency

The test was performed with two traffic load profiles as defined in the draft. Table 10 below describes the latency results measured with 50% of the maximum connection per second supported by the Firepower 4120.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	**avg**	**Max**	**Min**	**avg**	**Max**
1	1.8	3.1	58.8	<0.0009	1.6	53
16	1.8	3.3	61.4	1	4	63
64	1.9	3.8	65.8	2	6	78

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 the Firepower 4120.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	**avg**	**Max**	**Min**	**avg**	**Max**
1	1.9	3.2	59.3	<0.0009	0.9	52
16	1.9	3.9	61.8	1	2.5	56
64	1.9	4.3	65.5	2	3.9	68

Table 11: TCP/HTTPS TTFB and TTLB @ 50% of the maximum Throughput

Figures 4 -6 illustrate the distribution of maximum latency (TTFB and TTLB) values measured in approximately 75 measurement samples.
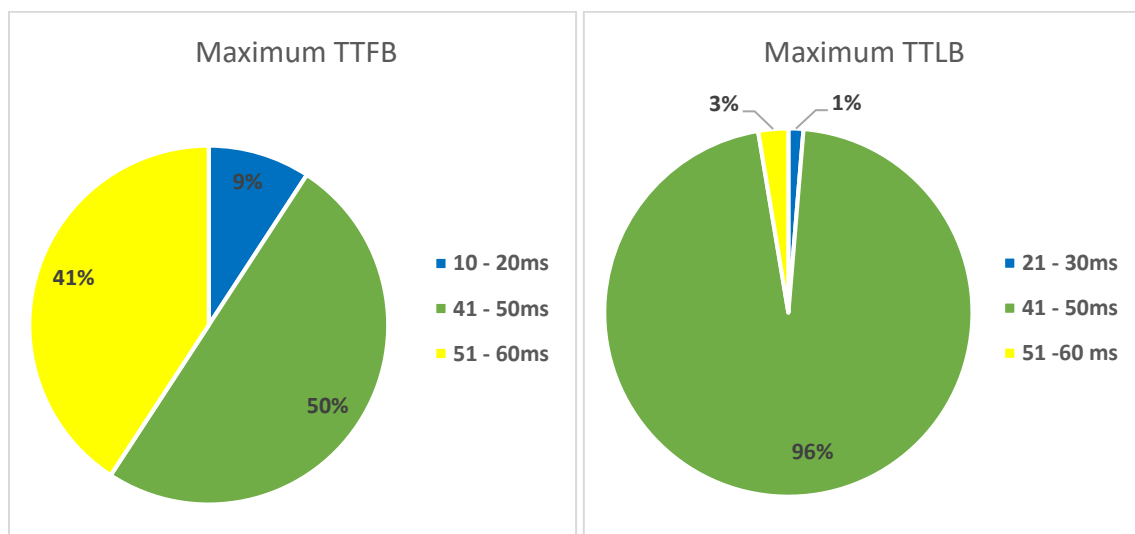

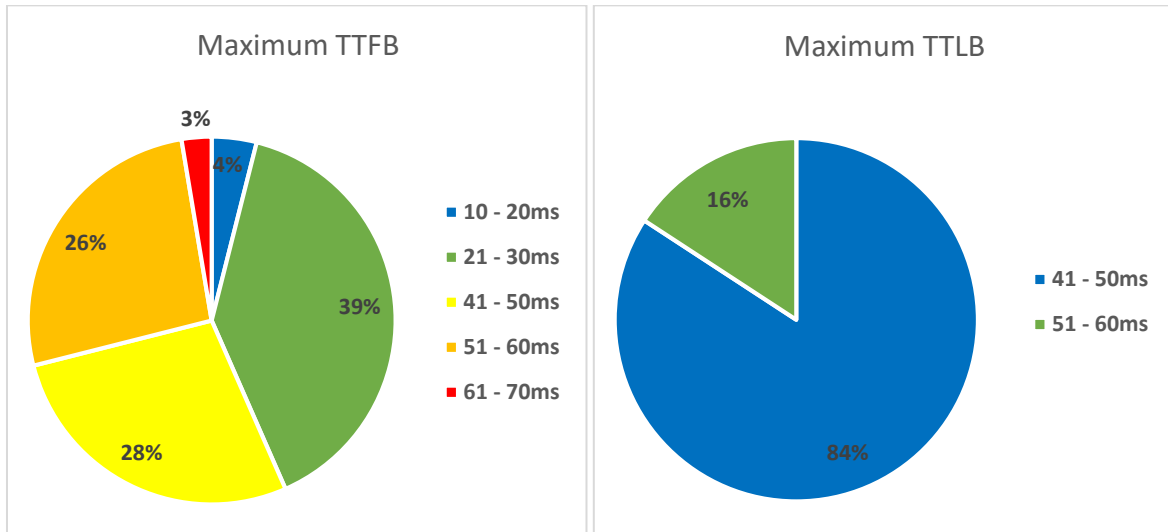*Figure 4:Latency distribution measured with 1KByte object size in Throughput test scenario*

Figure 5: Latency distribution measured with 16KByte object size in Throughput test scenario
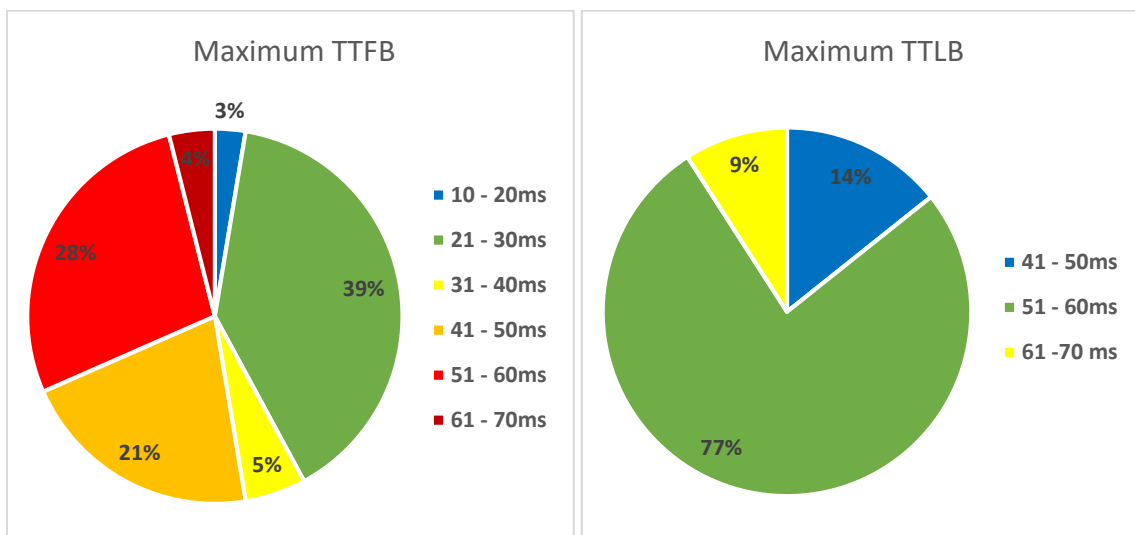

Figure 6:Latency distribution measured with 64KByte object size in Throughput test scenario

Concurrent TCP/HTTPS Connection Capacity

The Cisco Systems Firepower 4120 supported 145,440 concurrent TCP/HTTPS connections in average.
1 KByte object size was used as HTTPS GET request for each established TCP connection, which
resulted an average throughput of 20Mbit/s.