

NetSecOPEN Certification

Network Security Performance Testing

Palo Alto Networks PA-540 NGFW

Testing Information

Testing Information	
Vendor	Palo Alto
Product name and Model	PA-540 NGFW
Product version: Software	Software version: 12.1.4, Antivirus: 5468-5995, Applications and Threats: 9069-9910, WildFire:1068171-1072494
Test equipment(s)	Keysight PerfectStorm One
Test equipment version	PerfectStorm One: 26.0.0+2600.14 BreakingPoint and BreakingPoint Quick Test Version 26.0.40
Test Lab	University of New Hampshire Interoperability Lab
Test Date and Location	March 2026 Durham, NH

Table 1: Testing information

Tested based on [RFC 9411, Benchmarking Methodology for Network Security Device Performance.](#)

Executive Summary

Introduction

The goal of NetSecOPEN is to provide performance and security testing standards for the Network security products 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 their 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 PA-540 test report provided by the accredited test lab, the 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 Palo Alto Networks's PA-540 (version 12.1.4).

Note: This certification is product and version-specific.

Results Summary

This section describes the summary of the benchmarking performance tests and the security Effectiveness evaluation tests conducted based on [RFC 9411](#).

Performance Test

Tables 2-4 below show the measured values for Key Performance Indicators (KPIs) with different traffic. The KPI values for individual object sizes and test scenarios are described in the section. “Detailed Test Results”.

Application Traffic Mix Performance

TLS-Inspection feature was disabled on the PA-540 during the application Traffic mix performance test.

Note: Enabling this feature can potentially result in lower performance than the performance measured in these application Traffic mix performance test cases. However, for the remaining performance test cases, TLS Inspection was enabled.

Key Performance Indicator	Healthcare traffic mix ¹	Education traffic mix ¹
Inspected Throughput	1.45Gbit/s	1.44Gbit/s
Application Transactions per second	6,023	7,548

Table 2: Results summary for application mix traffic test

HTTP Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	5,998 CPS @ 1 KByte and 2,300 CPS @ 64 KByte object sizes
Inspected Throughput	1.62 Gbit/s @ 256 KByte and 0.11 Gbit/s @ 1 KByte object size
Transactions Per Second (TPS)	6,581 TPS @ 1 KByte and 740 TPS @ 256 KByte object size
Time to First Byte (TTFB)	1.26 ms average TTFB @ 1 KByte and 1.42 ms average TTFB @ 64 KByte object sizes ²
Time to Last Byte (TTLB)	1.25 ms average TTLB @ 1 KByte and 2.86 ms average TTLB @ 64 KByte object sizes ²
Concurrent connection	248,000 average concurrent connections

Table 3: Results summary for HTTP tests

HTTPS Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	899 CPS @ 1 KByte and 630 CPS @ 64 KByte object sizes
Inspected Throughput	1.20 Gbit/s @ 256 KByte and 0.06 Gbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	3,829 TPS @ 1 KByte and 546 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	2.50 ms average TTFB @ 1 KByte and 3.45 ms average TTFB @ 64 KByte object sizes ²
Time to Last Byte (TTLB)	2.50 ms average TTLB @ 1 KByte and 22.72 ms average TTLB @ 64 KByte object sizes ²
Concurrent connection	30,000 average concurrent connections

Table 4: Results summary for HTTPS tests

¹ The traffic mix profiles “Healthcare” and “Education” were defined by NetSecOPEN and the details can be found at <https://www.netsecopen.org/traffic-mixes>.

² Tested with 50% of max. inspected throughput that the PA-540 supported.

Security Effectiveness Tests

PA-540 blocked 5,376 Common Vulnerabilities and Exposures (CVE) out of 5,388, which is approximately 99.78%.

PA-540 maintained its threat detection and prevention capabilities while under load with both legitimate user traffic and malicious traffic. Details of the test scenarios are described in the section “**Detailed Test Results**”.

Test Setup and Configurations

All the tests were performed with the test setup (option 2) defined in [Section 4.1](#) of [RFC 9411](#). Six 1GbE interfaces of the PA-540 (DUT) were directly connected to the test equipment.

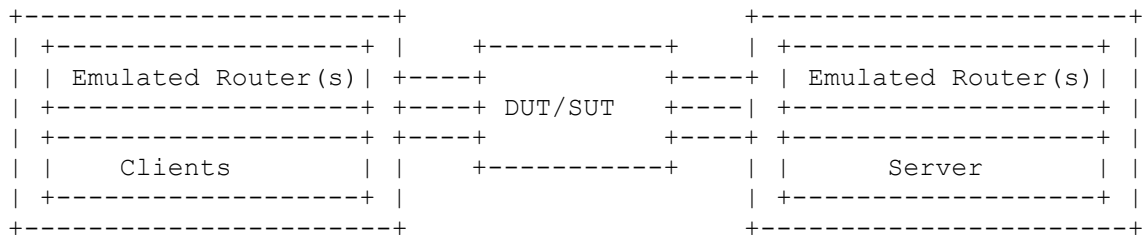


Figure 1: Testbed Setup

The table below shows the recommended and optional Next Generation Firewall (NGFW) features described in [Section 4.2](#) of [RFC 9411](#) that were enabled/disabled on the security device.

Features		Security device Status
TLS Inspection	Recommended	Enabled
IDS/IPS	Recommended	Enabled
Antivirus	Recommended	Enabled
Anti Spyware	Recommended	Enabled
Anti Botnet	Recommended	Enabled
Anti Evasion	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 5: NGFW security features

As defined in [Section 4.2](#) of [RFC 9411](#) (table 4, DUT classification “S”), 126 ACL rules were configured on the PA-540.

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.

Detailed Test Results

Throughput Performance with Application Traffic Mix

The test was performed with two different application traffic mix profiles, namely Healthcare and Education traffic profiles that were defined by NetSecOPEN. More details of the traffic profiles can be found at <https://www.netsecopen.org/traffic-mixes>.

Figures 2 and 3 below show the distribution of applications for Healthcare and Education traffic profiles.

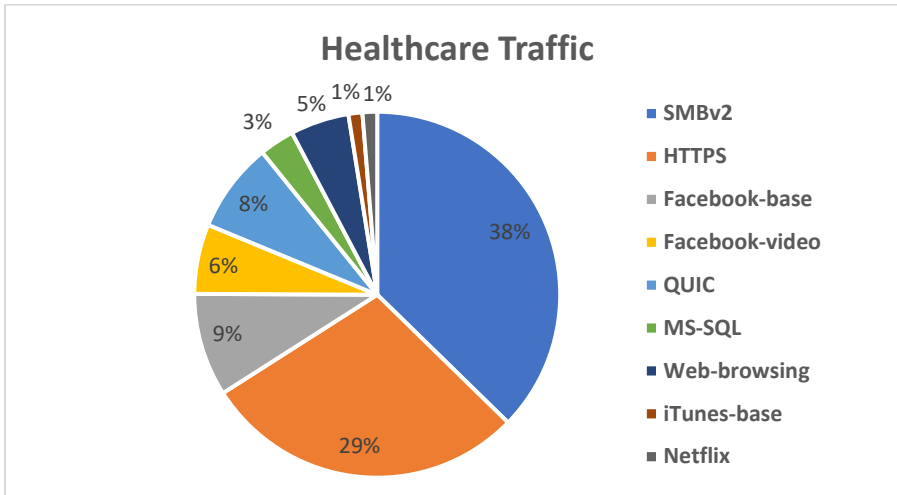


Figure 2: Healthcare Traffic Mix

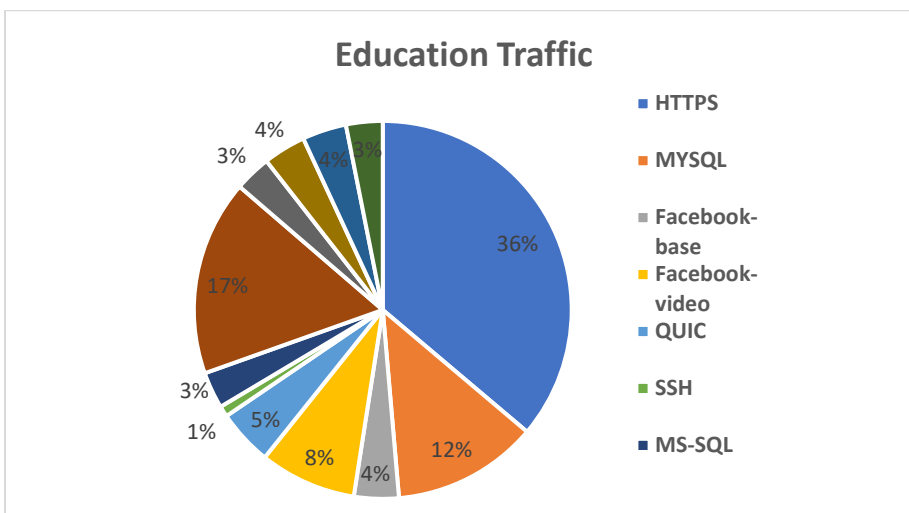


Figure 3: Education Traffic Mix

Table 6 below shows the tested KPIs and measured values by PA-540

Key Performance Indicator	Healthcare traffic mix	Education traffic mix
Inspected Throughput	1.45Gbit/s	1.44Gbit/s
Application Transactions per second	6,023	7,548

Table 6: Throughput performance with application mix traffic profiles

TCP Connections per Second with HTTP Traffic

Object Size [KByte]	Avg. TCP Connections Per Second
1	5,998
2	5,992
4	5,945
16	4,590
64	2,300

Table 7: TCP/HTTP Connections per Second

HTTP Throughput

Object Size [KByte]	Avg. HTTP Inspected Throughput [Gbit/s]	Avg. HTTP Transaction Per Second
1	0.11	6,581
16	0.69	4,798
64	1.28	2,318
256	1.62	740
Mixed objects	0.96	2,103

Table 8: HTTP Throughput

HTTP Transaction Latency

The test was performed with two traffic load profiles as defined in [RFC 9411](#). Table 9 below describes the latency results measured with 50% of the maximum connections per second supported by the PA-540.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	0.97	1.10	1.46	0.99	1.11	1.47
16	1.21	1.37	1.94	1.56	1.72	2.38
64	1.21	1.30	1.72	2.27	2.39	2.96

Table 9: TCP/HTTP TTFB and TTLB @ 50% of the maximum connection per second

Table 10 below describes latency results measured with 50% of the maximum throughput supported by the PA-540.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	1.18	1.26	1.69	1.77	1.25	1.69
16	1.23	1.31	1.79	1.55	1.64	2.17
64	1.30	1.42	1.84	2.72	2.86	3.44

Table 10: TCP/HTTP TTFB and TTLB @ 50% of the maximum Throughput

Concurrent TCP Connection Capacity with HTTP Traffic

The PA-540 supported 248,000 concurrent TCP connections on average. 1KByte object size was used as HTTP GET requests for each established TCP connection.

TCP Connections per Second with HTTPS Traffic

Object Size [KByte]	Avg. TCP/HTTPS Connections Per Second
1	899
2	880
4	850
16	770
64	630

Table 11: TCP/HTTPS Connections per Second

HTTPS Throughput

Object Size [KByte]	Avg. HTTPS Inspected Throughput [Gbit/s]	Avg. HTTPS Transaction Per Second
1	0.06	3,829
16	0.36	2,491
64	0.80	1,437
256	1.20	546
Mixed objects	0.74	1,619

Table 12: HTTPS Throughput

HTTPS Transaction Latency

The test was performed with two traffic load profiles as defined in the [RFC 9411](#). The latency results described below in Table 13 were measured with 50% of the maximum connections per second supported by the PA-540.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	3.51	4.13	5.72	3.65	4.27	5.86
16	3.98	4.48	7.69	95.47	96.10	100.21
64	4.22	4.72	6.16	186.48	187.63	189.96

Table 13: TCP/HTTPS TTFB and TTLB @ 50% of the maximum connection per second

The latency results below in Table 14 were measured with 50% of the maximum throughput supported by the PA-540.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	2.17	2.49	3.63	2.17	2.49	3.63
16	2.57	2.92	4.18	11.85	12.21	13.59
64	3.16	3.45	4.73	22.17	22.72	24.41

Table 14: TCP/HTTP TTFB and TTLB @ 50% of the maximum Throughput

Concurrent TCP Connection Capacity with HTTPS Traffic

The PA-540 supported 30,000 concurrent TCP connections on average. 1 KByte object size was used as HTTPS GET requests for each established TCP connection.

Security Effectiveness Tests

Two test scenarios were tested, namely the security effectiveness detection rate and the security effectiveness under load.

Security Effectiveness Detection Rate

This test was to verify that the PA-540 detects, prevents, and reports several types of attack scenarios. This test was performed without sending legitimate user traffic.

Table 15 below shows the results of this test:

Attack scenario	Number of tested attack scenarios	Blocked by PA-540	Blocked Rate (%)
Public Vulnerabilities³	1,380	1,368	99.13
Private Vulnerabilities⁴	180	180	100
Malware	3,809	3,809	100
Evasion Techniques	19	19	100

Table 15: Security Effectiveness Detection Rate

Security Effectiveness Under Load

The test was to verify that the PA-540 can maintain threat detection and prevention capabilities while the security engine of the PA-540 is under load with legitimate users and malicious traffic. In this test, the test equipment was configured to emulate the application traffic mix as legitimate traffic at the rate of 95% of the Maximum inspected throughput measured in the test scenario “**Throughput Performance with Application Traffic Mix**”. Simultaneously, the test equipment was configured to generate 50 CVEs from the public vulnerability set.

PA-540 security engine detected and reported all 50 CVEs while it was under load conditions.

Table 16 below shows the results in summary.

Generated Legitimate Traffic	Number of CVEs	Blocked CVEs	Not blocked CVEs
Healthcare Traffic mix at 1.37 Gbit/s (95% of maximum inspected Throughput)	50	50	0
Education Traffic mix at 1.37 Gbit/s (95% of maximum inspected Throughput)	50	50	0

Table 16: Security Effectiveness Under Load

Certification

After being reviewed by the NetSecOPEN Certification Body, PA-540 (version 12.1.4) was awarded certification in April 2026.

Note: This certification is specific to the product and version.

³ For the certification, NetSecOPEN provided the test labs with a list of public vulnerabilities (CVEs) to perform the security effectiveness test. The CVEs were selected according to the definition in section 4.2.1 of RFC 9411. The security device vendor knew about this CVE list before the test was started.

⁴ NetSecOPEN also provided the list of Private Vulnerabilities. However, the Security device vendor is unaware of this list.