NetSecOPEN Certification
Network Security Product Performance Testing
Palo Alto Networks PA-450 NGFW

Testing Information

Vendor: Palo Alto Networks

Product name and Model: PA-450 NGFW

Product version: 11.0.2-h2

Test Lab: University of New Hampshire Interoperability Lab

Test equipment: Keysight PerfectStorm One

Test equipment version: Firmware 9.20.2700.23, Application software 9.20.115.12, ATI 2023-17

Test Date and Location: November 2023 Durham, NH

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 test report of the PA-450 provided by the accredited test lab, 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-450 (Version 11.0.2-h2).
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.

Report template version: 1.1
Document: NetSecOPEN_Report_Palo_Alto_PA-450_(Version_11.0.2-h2)_v1.0
Created: February 2024

Performance Test

Table 1-3 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[1]

Key Performance Indicator	Healthcare traffic mix	Education traffic mix
Inspected Throughput	217 Mbit/s	239 Mbit/s
Application Transactions per second	865	1,185

Table 1: Results summary for application mix traffic test

HTTP Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	5,992 CPS @ 1 KByte and 1,300 CPS @ 64 KByte object sizes
Inspected Throughput	1,553 Mbit/s @ 256 KByte and 98 Mbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	8,333 TPS @ 1 KByte and 636 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	1.29 ms average TTFB @ 1 KByte and 1.46 ms average TTFB @ 64 KByte object sizes[2]
Time to Last Byte (TTLB)	1.29 ms average TTLB @ 1 KByte and 3.22 ms average TTLB @ 64 KByte object sizes[2]
Concurrent connection	298,900 average concurrent connection

Table 2: Results summary for HTTP tests

HTTPS Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	1,690 CPS @ 1 KByte and 780 CPS @ 64 KByte object sizes
Inspected Throughput	800 Mbit/s @ 256 KByte and 70 Mbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	4,966 TPS @ 1 KByte and 361 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	1.84 ms average TTFB @ 1 KByte and 3.51 ms average TTFB @ 64 KByte object sizes[2]
Time to Last Byte (TTLB)	1.84 ms average TTLB @ 1 KByte and 23.40 ms average TTLB @ 64 KByte object sizes[2]
Concurrent connection	30,000 average concurrent connection

Table 3: Results summary for HTTPS tests

Security Effectiveness Tests

PA-450 blocked 5447 Common Vulnerabilities and Exposures (CVE) out of 5470 which is approximately 99.58%.

PA-450 maintained threat detection or prevention capabilities while it was under load with legitimate user traffic and malicious traffic.

Details of the test scenarios are described in the section "**Detailed Test Results**".

[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-450 supported.

Test Setup and Configurations

All the tests were performed with the test setup (option 2) defined in Section 4.1 of RFC 9411. Four 1GbE interfaces of the PA-450 were directly connected with the test equipment.

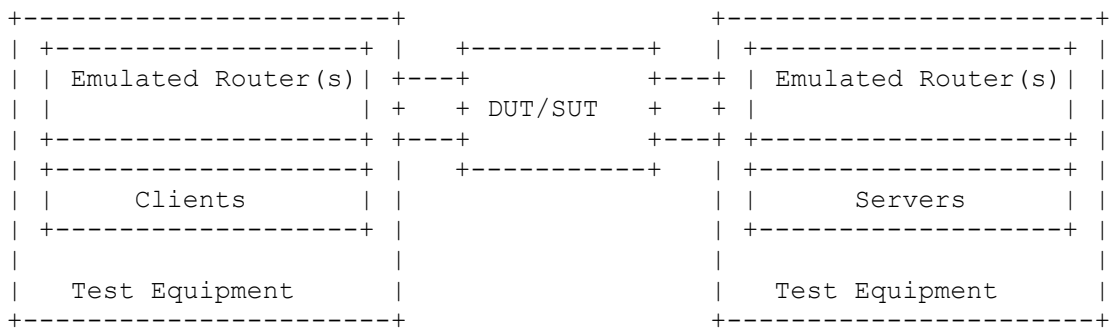

Figure 1: Testbed Setup

The table below shows the recommended and optional Next Generation Firewall (NGFW) features described in Section 4.2 of RFC 9411 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 4: NGFW security features

As defined in Section 4.2 of RFC 9411 (table 4, DUT classification “S”) 122 ACL rules were configured on the PA-450.

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.

During the test, it was observed that the tool would send Delayed ACKs later than expected. This caused retransmissions to be sent from the PA-450 and duplicate ACKs sent from the test tool resulting in the amount of received data to be larger than data transmitted. For this reason, the transmitted data rate was taken as the basis for measuring the inspected throughput. NetSecOPEN certification body has accepted this result since the number of application transaction failures of both traffic mixes were very minimal (Healthcare traffic mix had 5 transaction failures out of 654,174 and Education traffic mix had 2 transaction failures out of 922.279)

Note: For an update on this issue from UNH-IOL (the test lab), see the updated lab report at this link.

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

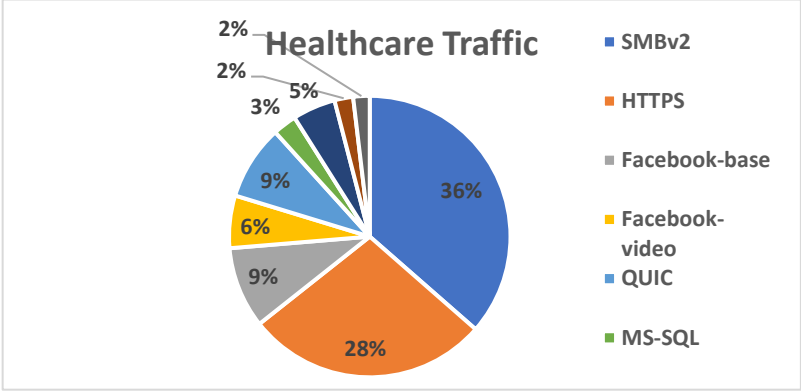

Figure 2: Healthcare Traffic Mix

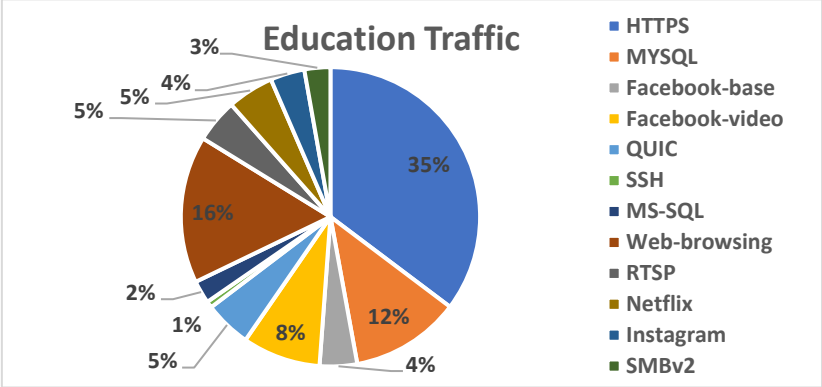

Figure 3: Education Traffic Mix

Table 5 below shows the tested KPIs and supported values by PA-450

Key Performance Indicator	Healthcare traffic mix	Education traffic mix
Inspected Throughput	217 Mbit/s	239 Mbit/s
Application Transactions per second	865	1,185

Table 5: Throughput performance with application mix traffic profiles

TCP Connections per Second with HTTP Traffic

Object Size [KByte]	Avg. TCP Connections Per Second
1	5,992
2	5,701
4	5,548
16	3,900
64	1,300

Table 6: TCP/HTTP Connections per Second

HTTP Throughput

Object Size [KByte]	Avg. HTTP Inspected Throughput [Mbit/s]	Avg. HTTP Transaction Per Second
1	98	8,333
16	679	4,860
64	1,049	1,900
256	1,553	636
Mixed objects	858	1,900

Table 7: HTTP Throughput

HTTP Transaction Latency

The test was performed with two traffic load profiles as defined in RFC 9411. Table 8 below describes the latency results measured with 50% of the maximum connection per second supported by PA-450.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	avg	Max
1	1.30	1.36	1.44	1.31	1.37	1.45
16	1.30	1.35	1.42	1.73	1.79	1.87
64	1.23	1.30	1.38	2.47	2.57	5.64

Table 8: TCP/HTTP TTFB and TTLB @ 50% of the maximum connection per second

Table 9 below describes latency results measured with 50% of the maximum throughput supported by PA-450.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	avg	Max
1	1.26	1.29	1.33	1.26	1.29	1.33
16	1.26	1.30	1.35	1.64	1.67	1.73
64	1.36	1.46	1.58	2.97	3.22	7.18

Table 9: TCP/HTTP TTFB and TTLB @ 50% of the maximum Throughput

Concurrent TCP Connection Capacity with HTTP Traffic

The PA-450 supported 298,900 concurrent TCP connections in average. 1 KByte object size was used as HTTP GET request for each established TCP connection.

TCP Connections per Second with HTTPS Traffic

Object Size [KByte]	Avg. TCP/HTTPS Connections Per Second
1	1,690
2	1,646
4	1,600
16	1,290
64	780

Table 10: TCP/HTTPS Connections per Second

HTTPS Throughput

Object Size [KByte]	Avg. HTTPS Inspected Throughput [Mbit/s]	Avg. HTTPS Transaction Per Second
1	70	4,966
16	413	2,900
64	662	1,200
256	800	361
Mixed objects	640	1,407

Table 11: HTTPS Throughput

HTTPS Transaction Latency

The test was performed with two traffic load profiles as defined in the RFC 9411. Table 12 below describes the latency results measured with 50% of the maximum connection per second supported by PA-450.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	avg	Max
1	1.93	2.04	2.16	2.10	2.21	2.42
16	2.48	2.63	3.41	92.76	93.06	93.79
64	3.19	3.43	4.76	183.88	184.40	185.65

Table 12: TCP/HTTPS TTFB and TTLB @ 50% of the maximum connection per second

Table 13 below describes latency results measured with 50% of the maximum throughput supported by PA-450.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	avg	Max
1	1.75	1.84	2.14	1.75	1.84	2.14
16	2.32	2.48	2.95	11.54	11.73	12.21
64	3.27	3.51	4.47	22.21	23.40	27.73

Table13: TCP/HTTP TTFB and TTLB @ 50% of the maximum Throughput

Concurrent TCP Connection Capacity with HTTPS Traffic

PA-450 supported 30,000 concurrent TCP connections in average. 1 KByte object size was used as HTTPS GET request for each established TCP connection.

Security Effectiveness Tests

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

Security Effectiveness Detection Rate

This test was to verify that PA-450 detects, prevents, and reports several types of attack scenarios. This test was performed without sending legitimate user traffic.

The table 14 below shows the results of this test:

Attack scenario	Number of tested attack scenarios	Blocked by PA-450	Blocked Rate (%)
Public Vulnerabilities[3]	1,381	1,360	98.48
Private Vulnerabilities[4]	180	178	98.89
Malware	3,809	3,809	100
Evasion Techniques	19	19	100

Table14: Security Effectiveness Detection Rate

Security Effectiveness Under Load

The test was to verify that the PA-450 can maintain threat detection and prevention capabilities while the security engine of the PA-450 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 93% 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-450's security engine detected and reported all 50 CVEs while it was under load conditions.

Table 15 below shows the results in summary.

Generated Legitimate Traffic	Number of CVEs	Blocked CVEs	Not blocked CVEs
Healthcare Traffic mix at 202 Mbit/s (93% of maximum inspected Throughput	50	50	0
Education Traffic mix at 220 Mbit/s (92% of maximum inspected Throughput	50	50	0

Table15: Security Effectiveness Under Load

Certification

As a result of review by the NetSecOPEN Certification Body certification is awarded to Palo Alto Networks's PA-450 NGFW (Version 11.0.2-h2) on February 2024.
Note: this certification is product and version-specific.

[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. This CVE list was known to the Security device vendor before the test was started.
[4] The list of Private Vulnerabilities was also provided by NetSecOPEN. However, this list is unknown to the Security device vendor.