NetSecOPEN Certification
Network Security Product Performance Testing
SonicWall NSa 4700

Testing Information

Testing Information	
Vendor	SonicWall
Product name and Model	SonicWall NSa 4700
Product version: Software	Software: SonicOS 7.0.1-6009
Test equipment	Spirent Cyberflood C100-S3
Test equipment version	Firmware: 5.47.3813 Software: 24.3.1012
Test Lab	University of New Hampshire Interoperability Lab
Test Date and Location	September 2024 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 SonicWall NSa 4700 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 SonicWall NSa 4700 (version SonicOS 7.0.1-6009).

Note: this certification is product and version-specific.

Report template version: 2.0
Document: NetSecOPEN_Report_SonicWall_NSa_4700(Version_7.0.1-6009)_v1.0
Created: October 2024

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[1]

Key Performance Indicator	Healthcare traffic mix	Education traffic mix
Inspected Throughput	958 Mbit/s	827 Mbit/s
Application Transactions per second	2,862	3,030

Table 2: Results summary for application mix traffic test

HTTP Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	30,510 CPS @ 1 KByte and 1,661 CPS @ 64 KByte object sizes
Inspected Throughput	6,521 Mbit/s @ 256 KByte and 1,293 Mbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	112,203 TPS @ 1 KByte and 3,043 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	0.49 ms average TTFB @ 1 KByte and 0.82 ms average TTFB @ 64 KByte object sizes[2]
Time to Last Byte (TTLB)	0.19 ms average TTLB @ 1 KByte and 0.78 ms average TTLB @ 64 KByte object sizes[2]
Concurrent connection	1,996,511 average concurrent connection

Table 3: Results summary for HTTP tests

HTTPS Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	2,200 CPS @ 1 KByte and 1,565 CPS @ 64 KByte object sizes
Inspected Throughput	3,289 Mbit/s @ 256 KByte and 296 Mbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	19,558 TPS @ 1 KByte and 1,520 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	5.14 ms average TTFB @ 1 KByte and 5.07 ms average TTFB @ 64 KByte object sizes[2]
Time to Last Byte (TTLB)	0.21 ms average TTLB @ 1 KByte and 0.86 ms average TTLB @ 64 KByte object sizes[2]
Concurrent connection	278,172 average concurrent connection

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 SonicWall NSa 4700 supported.

Security Effectiveness Tests

SonicWall NSa 4700 successfully blocked all 5,388 Common Vulnerabilities and Exposures (CVE).

SonicWall NSa 4700 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**".

Test Setup and Configurations

All the tests were performed with the test setup (option 2) defined in Section 4.1 of RFC 9411. Two 10GbE interfaces of the SonicWall NSa 4700 (DUT) were directly connected to the test equipment.

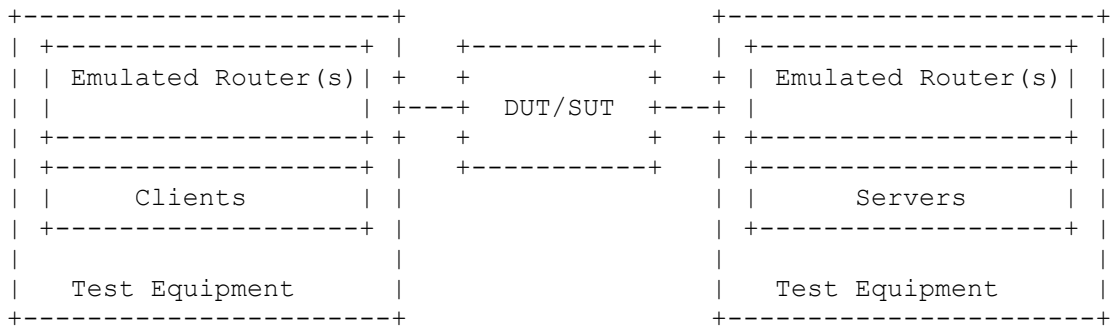

Figure 1: Testbed Setup

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 "M") 234 ACL rules were configured on the SonicWall NSa 4700.

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.

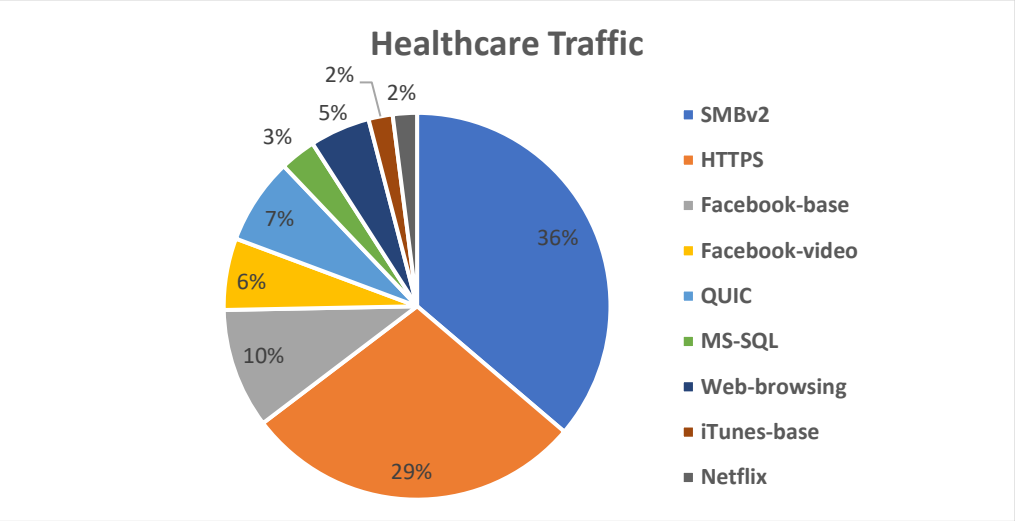

Figure 2: Healthcare Traffic Mix

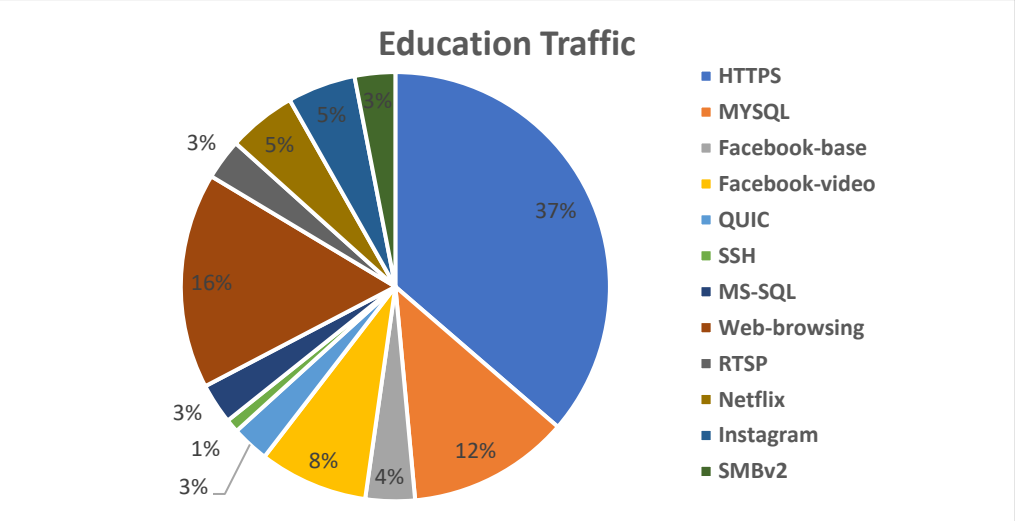

Figure 3: Education Traffic Mix

Table 6 below shows the tested KPIs and supported values by SonicWall NSa 4700

Key Performance Indicator	Healthcare traffic mix	Education traffic mix
Inspected Throughput	958 Mbit/s	827 Mbit/s
Application Transactions per second	2,862	3,030

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	30,510
2	22,180
4	14,982
16	5,324
64	1,661

Table 7: TCP/HTTP Connections per Second

HTTP Throughput

Object Size [KByte]	Avg. HTTP Inspected Throughput [Mbit/s]	Avg. HTTP Transaction Per Second
1	1,293	112,203
16	3,938	28,715
64	5,258	9,773
256	6,521	3,043
Mixed objects	5,694	12,874

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 connection per second supported by SonicWall NSa 4700.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	0.46	0.47	0.47	0.30	0.30	0.31
16	0.58	0.59	0.61	1.32	1.34	1.36
64	0.82	0.93	1.05	4.07	4.12	4.20

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 SonicWall NSa 4700.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	0.48	0.49	0.50	0.18	0.19	0.19
16	0.60	0.62	0.67	0.35	0.36	0.37
64	0.74	0.82	0.92	0.76	0.78	0.80

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

Concurrent TCP Connection Capacity with HTTP Traffic

The SonicWall NSa 4700 supported 1,996,511 concurrent TCP connections in average. 1 KByte 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	2,200
2	2,170
4	2,169
16	2,017
64	1,565

Table 11: TCP/HTTPS Connections per Second

HTTPS Throughput

Object Size [KByte]	Avg. HTTPS Inspected Throughput [Mbit/s]	Avg. HTTPS Transaction Per Second
1	296	19,558
16	1,671	11,869
64	2,820	5,168
256	3,289	1,520
Mixed objects	2,619	5,822

Table 12: HTTPS Throughput

HTTPS Transaction Latency

The test was performed with two traffic load profiles as defined in the RFC 9411. Table 13 The latency results described below were measured using 50% of the maximum connection per second supported by SonicWall NSa 4700.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	5.22	5.36	5.56	0.28	0.33	0.43
16	5.16	5.26	5.65	0.43	0.47	0.54
64	5.16	5.46	6.29	1.14	1.33	2.20

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

Table 14 The latency results below are measured with 50% of the maximum throughput supported by SonicWall NSa 4700.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	5.07	5.14	5.30	0.21	0.21	0.23
16	4.96	5.03	5.11	0.36	0.37	0.39
64	4.96	5.07	5.34	0.83	0.86	0.91

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

Concurrent TCP Connection Capacity with HTTPS Traffic

SonicWall NSa 4700 supported 278,172 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 security effectiveness detection rate and security effectiveness under load.

Security Effectiveness Detection Rate

This test was to verify that SonicWall NSa 4700 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 SonicWall NSa 4700	Blocked Rate (%)
Public Vulnerabilities[3]	1,380	1,380	100
Private Vulnerabilities[4]	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 SonicWall NSa 4700 can maintain threat detection and prevention capabilities while the security engine of the SonicWall NSa 4700 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 above the rate of 92% 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.

SonicWall NSa 4700 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 913 Mbit/s (95% of maximum inspected Throughput	50	50	0
Education Traffic mix at 763 Mbit/s (92% of maximum inspected Throughput	50	50	0

Table 16: Security Effectiveness Under Load

Certification

After being reviewed by the NetSecOPEN Certification Body, SonicWall NSa 4700 (Version: SonicOS 7.0.1-6009) was awarded certification in October 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. 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.