NetSecOPEN Certification
Network Security (SD-WAN) Performance Testing
Cisco Catalyst 8300 Edge Platform

Testing Information

Testing Information	
Vendor	Cisco
Product name and Model	SD-WAN Solution: Cisco C8300-2N2S-4T2X
Product version: Software	Cisco IOS XE Software, Version 17.12.04 Catalyst SD-WAN Manager, Version 20.13.1 Splunk Enterprise, Version 9.1.1
Test equipment	Keysight Ixia PerfectStorm One
Test equipment version	PerfectStorm One: 10.00.1000.14 Application: BreakingPoint, Version 10.00.1.74 BreakingPoint Quick Test, Version 10.00.10.47
Test Lab	University of New Hampshire Interoperability Lab
Test Date and Location	November 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 test report of the Cisco C8300-2N2S-4T2X 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 Cisco C8300-2N2S-4T2X (IOS XE Software Version 17.12.04).
Note: this certification is product and version-specific.

Report template version: 2.0
Document: NetSecOPEN_Report_Cisco_C8300-2N2S-4T2X_(IOS XE _17.12.04)_final)
Created: November 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

TLS-Inspection feature was disabled on the Cisco C8300-2N2S-4T2X 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 rest of performance testcases, TLS-Inspection was enabled.

Key Performance Indicator	Healthcare traffic mix[1]	Education traffic mix[1]
Inspected Throughput	3,421 Mbit/s	2,907 Mbit/s
Application Transactions per second	14,115	15,670

Table 2: Results summary for application mix traffic test

HTTP Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	18,069 CPS @ 1 KByte and 4,549 CPS @ 64 KByte object sizes
Inspected Throughput	3,699 Mbit/s @ 256 KByte and 465 Mbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	27,876 TPS @ 1 KByte and 1,691 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	2.01 ms average TTFB @ 1 KByte and 3.20 ms average TTFB @ 64 KByte object sizes[2]
Time to Last Byte (TTLB)	2.99 ms average TTLB @ 1 KByte and 5.55 ms average TTLB @ 64 KByte object sizes[2]
Concurrent connection	219,000 average concurrent connection

Table 3: Results summary for HTTP tests

HTTPS Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	129 CPS @ 1 KByte and 125 CPS @ 64 KByte object sizes
Inspected Throughput	243 Mbit/s @ 256 KByte and 22 Mbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	1,294 TPS @ 1 KByte and 110 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	7.18 ms average TTFB @ 1 KByte and 36.32 ms average TTFB @ 64 KByte object sizes[2]
Time to Last Byte (TTLB)	7.17 ms average TTLB @ 1 KByte and 290.18 ms average TTLB @ 64 KByte object sizes[2]
Concurrent connection	39,988 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 Cisco C8300-2N2S-4T2X supported.

Security Effectiveness Tests

Cisco C8300-2N2S-4T2X blocked 5,319 Common Vulnerabilities and Exposures (CVE) out of 5,388 which is approximately 98.8%.

Cisco C8300-2N2S-4T2X 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 Cisco C8300-2N2S-4T2X (DUT) were directly connected to the test equipment. In addition, the Cisco administration and management components, "Cisco SD-WAN Manager" and "Cisco SD-WAN App for Splunk," were connected to the DUT via the Internet. These components were hosted by Cisco On-Premises.

Note: Typically, SD-WAN solutions are used with overlay technology or protocols such as VXLAN, IPSec, or GRE. This can be configured between two SD-WAN sites (between two Cisco Catalyst 8300s). However, in this test setup, only one Catalyst 8300 was used and no overlay protocol was configured. Additionally, the Cisco SD-WAN Manager communicated with the DUT using the NETCONF protocol, via an SSH session.

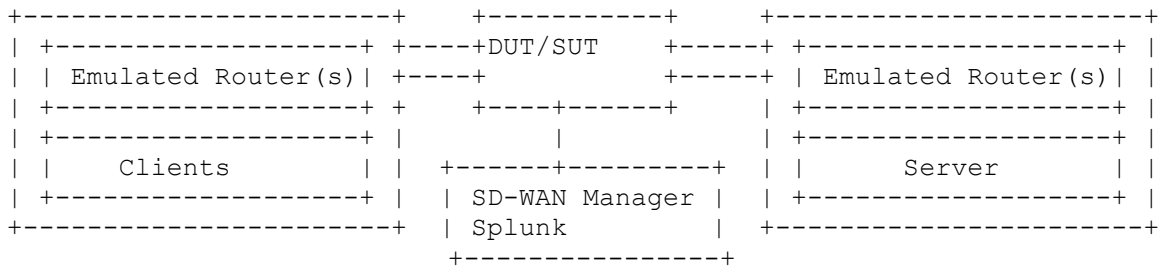

Figure 1: Testbed Setup

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 Cisco C8300-2N2S-4T2X.

Features		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") 124 ACL rules were configured on the Cisco C8300-2N2S-4T2X. 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. The TLS-Inspection feature was disabled on the Cisco C8300-2N2S-4T2X during both traffic mix performance tests.

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

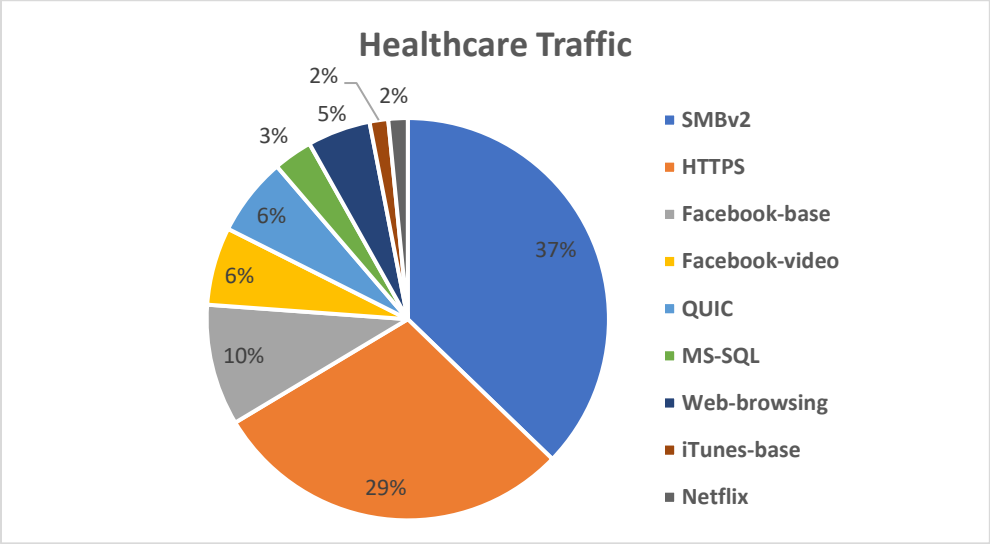

Figure 2: Healthcare Traffic Mix

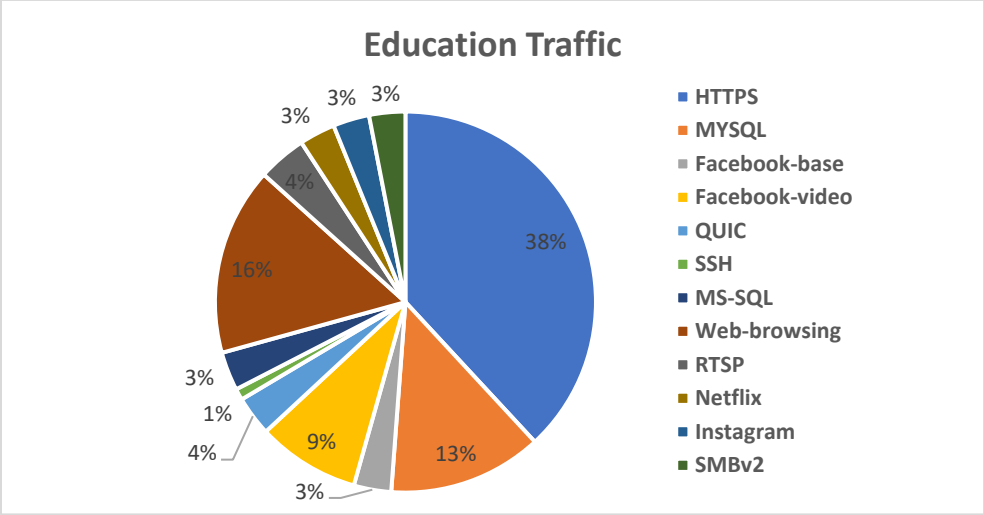

Figure 3: Education Traffic Mix

Table 6 below shows the tested KPIs and supported values by Cisco C8300-2N2S-4T2X

Key Performance Indicator	Healthcare traffic mix	Education traffic mix
Inspected Throughput	3,421 Mbit/s	2,907 Mbit/s
Application Transactions per second	14,115	15,670

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	18,069
2	16,784
4	15,276
16	8,523
64	4,549

Table 7: TCP/HTTP Connections per Second

HTTP Throughput

Object Size [KByte]	Avg. HTTP Inspected Throughput [Mbit/s]	Avg. HTTP Transaction Per Second
1	465	27,876
16	1,598	11,141
64	2,769	5,019
256	3,699	1,691
Mixed objects	2,784	6,125

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 Cisco C8300-2N2S-4T2X.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	0.94	1.11	1.28	0.95	1.12	1.29
16	1.99	1.30	1.42	1.33	1.42	1.54
64	1.35	1.59	1.77	1.47	1.70	1.87

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 Cisco C8300-2N2S-4T2X.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	1.93	2.01	2.12	2.90	2.99	3.14
16	3.26	3.40	3.56	5.81	5.90	5.99
64	3.06	3.20	3.31	5.47	5.55	5.64

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

Concurrent TCP Connection Capacity with HTTP Traffic

The Cisco C8300-2N2S-4T2X supported 219,000 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	129
2	130
4	131
16	128
64	125

Table 11: TCP/HTTPS Connections per Second

HTTPS Throughput

Object Size [KByte]	Avg. HTTPS Inspected Throughput [Mbit/s]	Avg. HTTPS Transaction Per Second
1	22	1,294
16	179	1,225
64	382	685
256	243	110
Mixed objects	387	843

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 Cisco C8300-2N2S-4T2X.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	0.74	0.93	1.16	0.74	0.94	1.17
16	0.92	1.09	1.44	1.86	2.09	2.48
64	1.15	1.37	1.65	63.67	68.02	74.75

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 Cisco C8300-2N2S-4T2X.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	6.69	7.18	7.66	6.69	7.17	7.66
16	16.43	18.15	19.27	17.99	19.27	19.94
64	26.15	36.32	47.65	276.41	290.18	303.22

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

Concurrent TCP Connection Capacity with HTTPS Traffic

Cisco C8300-2N2S-4T2X supported 39,988 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 Cisco C8300-2N2S-4T2X detects, prevents, and reports several types of attack scenarios. This test was performed without sending legitimate user traffic.

The Table 15 below shows the results of this test:

Attack scenario	Number of tested attack scenarios	Blocked by Cisco C8300-2N2S-4T2X	Blocked Rate (%)
Public Vulnerabilities[3]	1,380	1,349	97.75
Private Vulnerabilities[4]	180	178	98.88
Malware	3,809	3,779	99.21
Evasion Techniques	19	19	100

Table 15: Security Effectiveness Detection Rate

Security Effectiveness Under Load

The test was to verify that the Cisco C8300-2N2S-4T2X can maintain threat detection and prevention capabilities while the security engine of the Cisco C8300-2N2S-4T2X 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 94% 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.

Cisco C8300-2N2S-4T2X 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 3,220 Mbit/s (94% of maximum inspected Throughput	50	50	0
Education Traffic mix at 2,741 Mbit/s (94% of maximum inspected Throughput	50	50	0

Table 16: Security Effectiveness Under Load

Certification

After being reviewed by the NetSecOPEN Certification Body, Cisco C8300-2N2S-4T2X (IOS XE Software, Version 17.12.04) was awarded certification in December 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.