NetSecOPEN Certification
Network Security Product Performance Testing
Fortinet FortiGate 601F NGFW

Testing Information

Vendor: Fortinet

Product name and Model: FortiGate 601F NGFW

Product version: v7.2.6,build1575,230926 (GA.F)

Test Lab: EANTC AG

Test equipment: Spirent Cyberflood C100-S3

Test equipment version: 5.44.3243

Test Date and Location: December 2023 Berlin, Germany

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 FortiGate 601F provided by the accredited test lab, EANTC AG. These results have been found to meet the NetSecOPEN certification requirements. Detailed results are provided below.

NetSecOPEN Certification is awarded to Fortinet's FortiGate-601F (v7.2.6,build1575,230926 (GA.F)).
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.

© NetSecOPEN 2024 All Rights Reserved
Report template version: 1.1
Document: NetSecOPEN_Report_Fortinet_FortiGate-601F_(Version_7.2.6)_v1.
Created: 1-Feb-24

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	808.81 Mbit/s	798.21 Mbit/s
Application Transactions per second	2,743	3,208

Table 1: Results summary for application mix traffic test

HTTP Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	6,700 CPS @ 1 KByte and 2,106 CPS @ 64 KByte object sizes
Inspected Throughput	3,791 Mbit/s @ 256 KByte and 222 Mbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	19,325 TPS @ 1 KByte and 1,775 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	1.61 ms average TTFB @ 1 KByte and 1.64 ms average TTFB @ 64 KByte object sizes[2]
Time to Last Byte (TTLB)	0.79 ms average TTLB @ 1 KByte and 2.72 ms average TTLB @ 64 KByte object sizes[2]
Concurrent connection	1,340,000 average concurrent connection

Table 2: Results summary for HTTP tests

HTTPS Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	2,742 CPS @ 1 KByte and 1,384 CPS @ 64 KByte object sizes
Inspected Throughput	3,484 Mbit/s @ 256 KByte and 203 Mbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	15,205 TPS @ 1 KByte and 1,625 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	2.79 ms average TTFB @ 1 KByte and 2.78 ms average TTFB @ 64 KByte object sizes[2]
Time to Last Byte (TTLB)	1.16 ms average TTLB @ 1 KByte and 3.24 ms average TTLB @ 64 KByte object sizes[2]
Concurrent connection	657,000 average concurrent connection

Table 3: Results summary for HTTPS tests

Security Effectiveness Tests

FortiGate 601F blocked 5,208 Common Vulnerabilities and Exposures (CVE) out of 5,209 which is approximately 99.98%.

FortiGate 601F 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 FortiGate 601F supported.

© NetSecOPEN 2024 All Rights Reserved

Test Setup and Configurations

All the tests were performed with the test setup (option 2) defined in Section 4.1 of RFC 9411. Four 10GbE interfaces of the FortiGate 601F were directly connected with the test equipment.

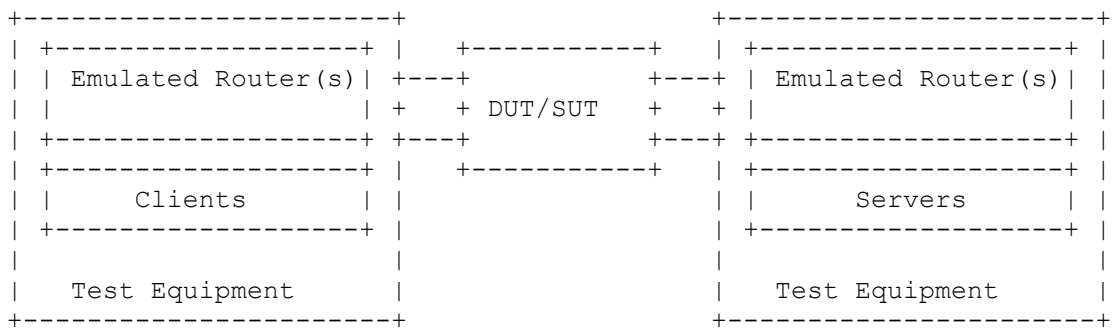

Figure 1: Testbed Setup

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
TLS 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 "L") 568 ACL rules were configured on the FortiGate 601F.

All tests were performed with IPv4 traffic only. The **ECDHE-RSA-AES128-GCM-SHA256 with Prime256v1** cipher suite was used for all the HTTPS performance tests.

© NetSecOPEN 2024 All Rights Reserved

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.

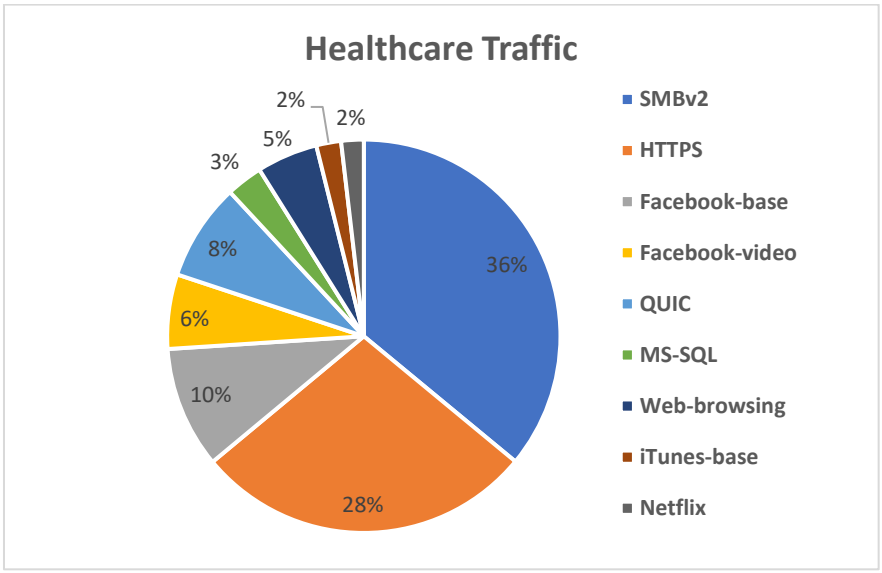

Figure 2: Healthcare Traffic Mix

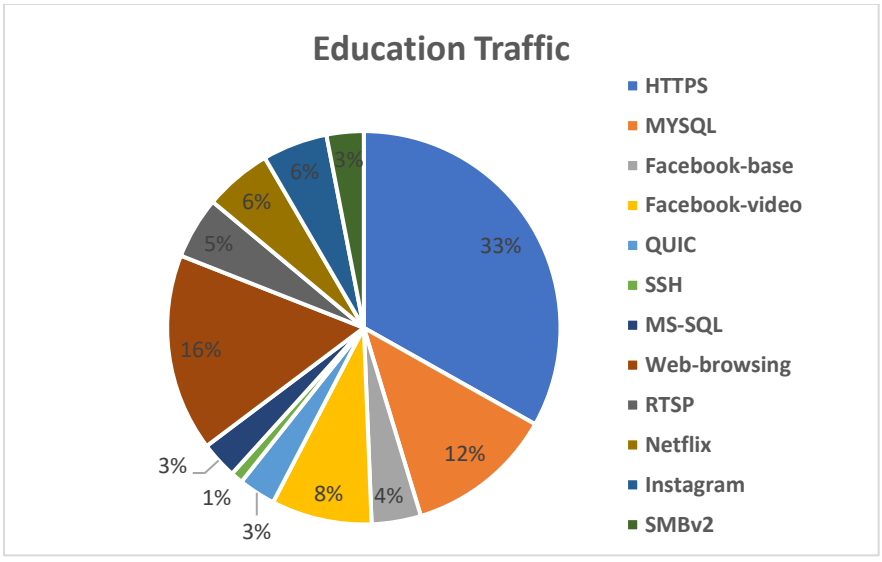

Figure 3: Education Traffic Mix

Table 5 below shows the tested KPIs and supported values by FortiGate 601F

Key Performance Indicator	Healthcare traffic mix	Education traffic mix
Inspected Throughput	808.81 Mbit/s	798.21 Mbit/s
Application Transactions per second	2,743	3,208

Table 5: Throughput performance with application mix traffic profiles

© NetSecOPEN 2024 All Rights Reserved

TCP Connections per Second with HTTP Traffic

Object Size [KByte]	Avg. TCP Connections Per Second
1	13,390
2	11,572
4	9,792
16	7,397
64	4,206

Table 6: TCP/HTTP Connections per Second

HTTP Throughput

Object Size [KByte]	Avg. HTTP Inspected Throughput [Mbit/s]	Avg. HTTP Transaction Per Second
1	222	19,325
16	1,275	9,324
64	2,668	4,977
256	3,791	1,775
Mixed objects	2,529	5,740

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 FortiGate 601F.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	1.41	1.76	4.30	0.94	1.06	3.42
16	1.21	1.73	2.38	1.86	2.19	5.90
64	1.26	1.66	2.06	3.53	3.93	7.91

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 FortiGate 601F.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	1.32	1.61	6.09	0.73	0.79	1.57
16	1.09	1.28	1.69	1.30	1.33	2.33
64	1.29	1.64	2.71	2.57	2.72	3.81

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

Concurrent TCP Connection Capacity with HTTP Traffic

The FortiGate 601F supported 1,340,000 concurrent TCP connections in average. 1 KByte object size was used as HTTP GET request for each established TCP connection.

© NetSecOPEN 2024 All Rights Reserved

TCP Connections per Second with HTTPS Traffic

Object Size [KByte]	Avg. TCP/HTTPS Connections Per Second
1	5,463
2	5,035
4	4,722
16	3,970
64	2,764

Table 10: TCP/HTTPS Connections per Second

HTTPS Throughput

Object Size [KByte]	Avg. HTTPS Inspected Throughput [Mbit/s]	Avg. HTTPS Transaction Per Second
1	203	15,205
16	1,130	8,125
64	2,325	4,313
256	3,484	1,625
Mixed objects	2,321	5,232

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 FortiGate 601F.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	2.43	2.68	3.11	1.64	1.75	5.74
16	2.32	2.59	3.22	2.36	2.52	7.29
64	2.32	2.57	3.05	3.74	3.98	6.63

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 FortiGate 601F.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	2.02	2.79	4.26	1.10	1.16	1.85
16	2.09	2.54	3.06	1.75	1.81	2.50
64	2.20	2.78	4.30	3.08	3.24	4.17

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

Concurrent TCP Connection Capacity with HTTPS Traffic

FortiGate 601F supported 657,000 concurrent TCP connections in average. 1 KByte object size was used as HTTPS GET request for each established TCP connection.

© NetSecOPEN 2024 All Rights Reserved

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 FortiGate 601F 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 FortiGate 601F	Blocked Rate (%)
Public Vulnerabilities[3]	1,381	1,380	99.92
Private Vulnerabilities[4]	180	180	100
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 FortiGate 601F can maintain threat detection and prevention capabilities while the security engine of the FortiGate 601F is under load with legitimate users and malicious traffic. In this test, the test equipment was configured to emulate HTTP as legitimate traffic at the rate of 95% of the Maximum inspected throughput measured in the test scenario **HTTP Throughput**. Simultaneously the test equipment was configured to generate 50 CVEs from the public vulnerability set.

FortiGate 601F'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
HTTP traffic with 64 KByte object size at 2,535 Mbit/s	50	50	0

Table15: Security Effectiveness Under Load

Certification

As a result of review by the NetSecOPEN Certification Body certification is awarded to Fortinet's FortiGate 601F NGFW (Version v7.2.6,build1575,230926 (GA.F)) on January 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.

© NetSecOPEN 2024 All Rights Reserved