NetSecOPEN Certification
Network Security Product Performance Testing
TippingPoint 8600TXE

Testing Information

Testing Information	
Vendor	Trend Micro
Product name and Model	Security device: TippingPoint 8600TXE (Next Generation IPS) Controller: Security Management System
Product version: Software	Software: TOS 6.3.0.13244, Digital Vaccine: 4.0.0.9956, Auxiliary DV's: Malware 3.7.0.2009, Controller Firmware: 6.3.0.207000.1
Test equipment	Keysight XGS2-HSL: for Performance test Spirent Cyberflood C200: for Traffic mix and security effectiveness test
Test equipment version	XGS2-HSL: BreakingPoint 10.00.1.74, Cyberflood C200: 5.50.4353
Test Lab	University of New Hampshire Interoperability Lab
Test Date and Location	January 2025 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 TippingPoint 8600TXE 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 TippingPoint 8600TXE (version TOS 6.3.0.13244).

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 TippingPoint 8600TXE 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 test cases, TLS-Inspection was enabled.

Key Performance Indicator	Healthcare traffic mix[1]	Education traffic mix[1]
Inspected Throughput	30.16 Gbit/s	27.75 Gbit/s
Application Transactions per second	112,408	127,801

Table 2: Results summary for application mix traffic test

HTTP Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	999,923 CPS @ 1 KByte and 83,979 CPS @ 64 KByte object sizes
Inspected Throughput	50.27 Gbit/s @ 256 KByte and 28.03 Gbit/s @ 1 KByte object size
Transactions Per Second (TPS)	1,679,864 TPS @ 1 KByte and 23,000 TPS @ 256 KByte object size
Time to First Byte (TTFB)	0.10 ms average TTFB @ 1 KByte and 0.20 ms average TTFB @ 64 KByte object sizes[2]
Time to Last Byte (TTLB)	0.14 ms average TTLB @ 1 KByte and 0.86 ms average TTLB @ 64 KByte object sizes[2]
Concurrent connection	240,000,000 average concurrent connections

Table 3: Results summary for HTTP tests

HTTPS Traffic Performance

Key Performance Indicator	Values
Connections Per Second (CPS)	19,102 CPS @ 1 KByte and 14,717 CPS @ 64 KByte object sizes
Inspected Throughput	39.08 Gbit/s @ 256 KByte and 2.52 Gbit/s @ 1 KByte object sizes
Transactions Per Second (TPS)	149,966 TPS @ 1 KByte and 17,755 TPS @ 256 KByte object sizes
Time to First Byte (TTFB)	0.12 ms average TTFB @ 1 KByte and 0.19 ms average TTFB @ 64 KByte object sizes[2]
Time to Last Byte (TTLB)	0.41 ms average TTLB @ 1 KByte and 2.65 ms average TTLB @ 64 KByte object sizes[2]
Concurrent connection	250,000 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 TippingPoint 8600TXE supported.

Security Effectiveness Tests

TippingPoint 8600TXE blocked 1,549 Common Vulnerabilities and Exposures (CVE) out of 1,579.

TippingPoint 8600TXE 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 40 GbE interfaces of the TippingPoint 8600TXE (DUT) were directly connected to the test equipment. In addition, the security Management System was connected to the DUT directly.

```
+------------------------+    +------------+      +------------------------+
| +--------------------+ +-----+DUT/SUT     +------+ +--------------------+ |
| | Emulated Router(s) | +-----+            +------+ | Emulated Router(s) | |
| +--------------------+ +    +----+-------+      | +--------------------+ |
| +--------------------+ |         |              | +--------------------+ |
| |     Clients        | |   +-------+----------+ | |       Server       | |
| +--------------------+ |   | Security         | | +--------------------+ |
+------------------------+   | Management       | +------------------------+
                             | System           |
                             +------------------+
```

Figure 1: Testbed Setup

The table below shows the recommended and optional Next Generation IPS (NGIPS) 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
Anti-malware	Recommended	Enabled
Anti-Spyware	Recommended	Enabled
Anti-Botnet	Recommended	Enabled
Application Identification	Recommended	Enabled
Deep Packet Inspection (DPI)	Recommended	Enabled
Anti Evasion	Recommended	Enabled
Logging and Reporting	Recommended	Enabled

Table 5: NGFW security features

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.

Note 1: The TLS-Inspection feature was disabled on the TippingPoint 8600TXE during both traffic mix performance tests.

Note 2: During the test, the test tool hit its performance limitation, and therefore, the throughput rate could not be increased on the test tool. Due to the test tool limitation, the maximum sustainable inspected throughput supported by the DUT could not be measured.

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

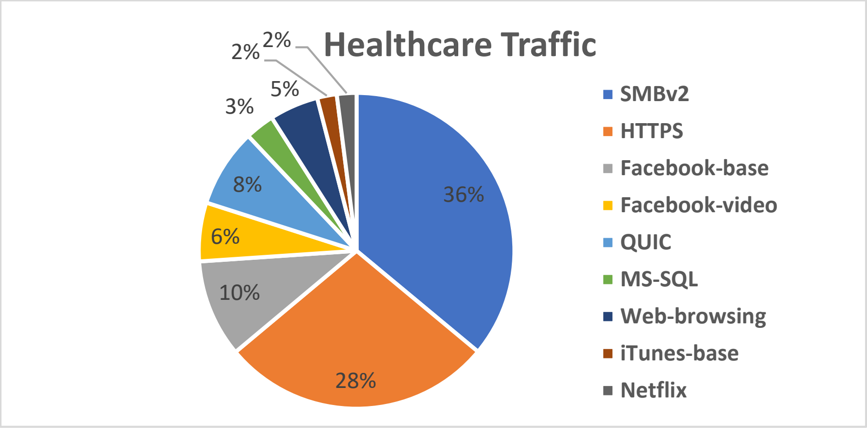

Figure 2: Healthcare Traffic Mix

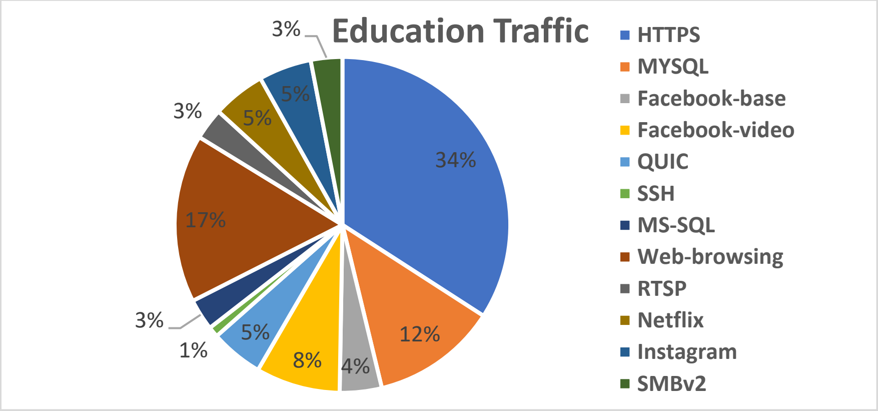

Figure 3: Education Traffic Mix

Table 6 below shows the tested KPIs and measured values by TippingPoint 8600TXE

Key Performance Indicator	Healthcare traffic mix	Education traffic mix
Inspected Throughput	30.16 Gbit/s	27.75 Gbit/s
Application Transactions per second	112,408	127,801

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	999,923
2	837,090
4	697,412
16	293,968
64	83,979

Table 7: TCP/HTTP Connections per Second

HTTP Throughput

Object Size [KByte]	Avg. HTTP Inspected Throughput [Gbit/s]	Avg. HTTP Transaction Per Second
1	28.03	1,679,864
16	47.46	329,916
64	48.00	86,866
256	50.26	23,000
Mixed objects	48.83	107,440

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 TippingPoint 8600TXE.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	0.06	0.07	0.07	0.13	0.14	0.15
16	0.07	0.08	0.08	0.26	0.27	0.29
64	0.07	0.08	0.08	0.79	0.83	0.86

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 TippingPoint 8600TXE.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	0.10	0.10	0.10	0.14	0.14	0.14
16	0.12	0.12	0.12	0.28	0.28	0.28
64	0.18	0.20	0.22	0.82	0.86	0.90

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

Concurrent TCP Connection Capacity with HTTP Traffic

In this test, the test tool was able to emulate a maximum value of 240,000,000 concurrent TCP connections. Due to the limitations of the test tool, the test lab could verify that the TippingPoint 8600TXE can support 240,000,000 concurrent TCP connections. However, TippingPoint 8600TXE could theoretically sustain an increased amount of concurrent TCP connections.

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	19,102
2	19,023
4	18,832
16	18,007
64	14,717

Table 11: TCP/HTTPS Connections per Second

HTTPS Throughput

Object Size [KByte]	Avg. HTTPS Inspected Throughput [Gbit/s]	Avg. HTTPS Transaction Per Second
1	2.52	149,966
16	17.32	119,973
64	28.91	51,513
256	39.08	17,755
Mixed objects	30.80	67,394

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 TippingPoint 8600TXE.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	0.41	0.44	0.50	0.33	0.36	0.41
16	0.63	0.68	0.73	0.40	0.45	0.49
64	0.59	0.64	0.69	0.57	0.62	0.67

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 TippingPoint 8600TXE.

Object Size [KByte]	Time to First Byte [ms]			Time to Last Byte [ms]		
	Min	avg	Max	Min	Avg	Max
1	0.11	0.12	0.14	0.38	0.41	0.43
16	0.25	0.27	0.28	0.53	0.56	0.59
64	0.18	0.19	0.21	2.38	2.65	3.01

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

Concurrent TCP Connection Capacity with HTTPS Traffic

TippingPoint 8600TXE supported 250,000 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 security effectiveness detection rate and security effectiveness under load.

Security Effectiveness Detection Rate

This test was to verify that TippingPoint 8600TXE detects, prevents, and reports several types of attack scenarios. This test was performed without sending legitimate user traffic.

The TippingPoint 8600TXE specializes in detecting and preventing Command and Control (C&C) attacks. NetSecOPEN's malware definitions contain common malware samples that are sent pre-infection as a payload for the DUT/SUT to detect and prevent. C&C attacks post-infection are currently not included in the scenario tested. The vendor has requested that we omit the pre-infection malware attack scenario from this test.

Table 15 below shows the results of this test:

Attack scenario	Number of tested attack scenarios	Blocked by TippingPoint 8600TXE	Blocked Rate (%)
Public Vulnerabilities[3]	1,380	1,354	98.12
Private Vulnerabilities[4]	180	176	98.78
Malware	0	N/A	N/A
Evasion Techniques	19	19	100

Table 15: Security Effectiveness Detection Rate

Security Effectiveness Under Load

The test was to verify that the TippingPoint 8600TXE can maintain threat detection and prevention capabilities while the security engine of the TippingPoint 8600TXE 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 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.

TippingPoint 8600TXE 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 28.7 Gbit/s (95% of maximum inspected Throughput	50	50	0
Education Traffic mix at 26.48 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, TippingPoint 8600TXE **(Version: 6.3.0.13244) was awarded certification in March 2025.**

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.