Unified Threat Management
Comparative Throughput Performance

WatchGuard Firebox M370

SonicWALL NSA 2600

Fortinet FortiGate 100E

Sophos XG 210

July 2017

DR170718B

Miercom.com

www.miercom.com

Contents

Executive Summary

Unified Threat Management (UTM) appliances contain the security functionality of next-generation firewalls and secure web gateways but are designed for more granular control of small and mid-size business networks. A common problem with secure traffic processing is the degradation of throughput performance. With more security features enabled, the throughput rate decreases. Performance testing of UTM products helps identify which security services cause the worst throughput during high volume traffic scenarios.

Miercom was engaged by WatchGuard Technologies, Inc. to conduct an independent, comparative performance assessment of its Firebox M370 against similar leading UTM network security appliances: SonicWALL NSA 2600, Fortinet FortiGate 100E and Sophos XG 210. All products were exposed to increasing traffic loads, with different protocols, while evaluating the impact on network performance.

Product comparisons were made using the following scenarios: baseline firewall, additional security features and full UTM mode. Firewall performance measured transport and application network layer traffic. Then security features were individually enabled to evaluate the impact on performance for HTTP and HTTPS loads. Finally, the full set of security functions was enabled (firewall, intrusion prevention system, antivirus and application control) over HTTP and HTTPS.

Key Findings

- **Highest stateless traffic performance.** Firebox M370 achieved the maximum throughput for stateless traffic at 6 Gbps for UDP 1518-byte packets and 4.1 Gbps for realistic UDP IMIX, exceeding competitive rates by as much as 94 percent.
- **Most stateful HTTP throughput.** The highest throughput was maintained for baseline and full security enabled, beating its competitors by as much as 94 percent.
- **Superior encrypted traffic rates.** With 960 Mbps throughput for baseline and 820 Mbps with full security for HTTPS traffic, the Firebox M370 provided 3 times more throughput.

Based on results of our testing, the WatchGuard Firebox M370 displayed exceptional performance, outperforming its competitors for stateless and stateful traffic throughput scenarios. Its high-rate performance with security features enabled earns it the ***Miercom Performance Verified*** certification.

Robert Smithers

CEO

Miercom

Introduction

Unified Threat Management devices are an evolving class of network edge security platforms that incorporate and perform multiple security functions in a single appliance. The devices tested for this report all address and incorporate the security functions below.

Security Function	Acronym	Description
Firewall	FW	Controls and filters the flow of traffic, providing a relatively low-level barrier to protect a trusted internal network from an unsecure network (such as the Internet).
Intrusion Prevention System	IPS	Monitors all network activity, looking for malicious behavior based on known-threat signatures, statistical anomalies, or stateful protocol analysis. If malicious or highly suspicious packets are detected, they are identified, logged, reported and, depending on IPS settings, automatically blocked from access to the internal network.
Application Control	AppCtrl	Enforces policies regarding security and resources (network bandwidth, servers, etc.) by restricting or controlling which application traffic can pass through the UTM, usually in either direction. Security-wise, Application Control is intended to reduce occurrences of infection, attacks and malicious content.
Hypertext Transfer Protocol Proxy/Antivirus	HTTP Proxy/AV	The security appliance is a proxy for HTTP traffic. This is where a client issues a "get" request and retrieved files are buffered in memory in the security appliance. Files are then sent to an antivirus engine that looks for viruses and removes packets containing malicious content. Proxy-based virus and content scanning is a more secure and accurate method than stream-based inspection of client/server traffic. With Proxy/AV scanning is performed during the handshake of data transfer.
Hypertext Transfer Protocol Secure	HTTPS	The security device responds to incoming encrypted connection requests on the secure socket layer (SSL), and then actively scans and blocks packets containing malicious content, similar to HTTP/AV processing. The HTTPS encryption/decryption process places an appreciable load on the security device that directly impacts its overall throughput rate.
Unified Threat Management	UTM	An all-inclusive security setting, where multiple functions are performed by the same, single security device. The functions typically include: firewall, IPS, AV, VPN (control of virtual private network tunnels), content filtering, and sensitive data loss prevention.

Products Tested

Product	Firmware Version
WatchGuard Firebox M370	11.12.4
SonicWALL NSA 2600	6.2.7.1-23n
Fortinet FortiGate 100-E	5.6.0 B1449
Sophos XG 210	16.05.4 MR-4

WatchGuard Firebox M370

The *Firebox M370* is the latest and powerful offering in WatchGuard's Firebox UTM series. It offers enterprise-grade security to small and mid-size businesses with eight 1-GE ports. Its firewall throughput is specified to reach a maximum of 8 Gbps.

Supported security features include: firewall, virtual private networking with SSL and IPSec, intrusion prevention, application proxies for various protocols (HTTPS, HTTPS, SMTP, DNS and others) and antivirus. Routing is policy based, and reporting is simple.

SonicWALL Network Security Appliance (NSA) 2600

The *SonicWALL NSA 2600* is a simple but effective next generation firewall for securing small businesses, branch offices and campuses. Its eight 1-GE ports support a firewall throughput of up to 1.9 Gbps.

Supported security features include: deep packet inspection firewall, stateful packet inspection firewall, application intelligence and control, intrusion prevention, antivirus, antispyware, content and URL filtering and SSL inspection.

Fortinet FortiGate 100E

The *FortiGate 100E* is an enterprise-grade firewall solution for unified security and policy management. There are twenty ports – 2 WAN, 1 DMZ, 1 Management, 2 High Availability, and 14 Switch ports. It is specified to provide throughput of up to 7.4 Gbps for firewall, 500 Mbps for IPS and 360 Mbps for UTM.

Supported security features include: firewall policies, virtual private networking with SSL and IPSec, intrusion prevention, application control and next generation firewall.

Sophos XG 210

The *Sophos XG 210* firewall provides a unified management system to create policies based on user and applications for powerful network protection, with six ports to support up to 14 Gbps of firewall throughput and 1.7 Gbps next generation firewall performance.

Supported security features include: firewall, virtual private networking, intrusion prevention, application control, web filtering and antivirus.

How We Did It

Miercom used hands-on testing designed to simulate real-world threat environments, providing a robust, realistic assessment of product capability and effectiveness. The methodology used in testing consisted of a framework of tests for validating the throughput of each Device Under Test (DUT).

Traffic generation was fundamental to throughput testing and determination of processing capabilities for each DUT. Realistic UDP, HTTP and HTTPS traffic flows were produced and circulated through the test network to simulate typical client-server requests and file transfers.

To determine the effect of security features on throughput, we began with a baseline test. As some devices are unable to disable firewall inspection, the baseline test evaluated firewall functionality. This low-level traffic processing feature represented the highest achievable throughput for each UTM device. The resulting rate was used in comparison for throughput results where additional security services were enabled to identify which feature placed the greatest load and which UTM was the most affected.

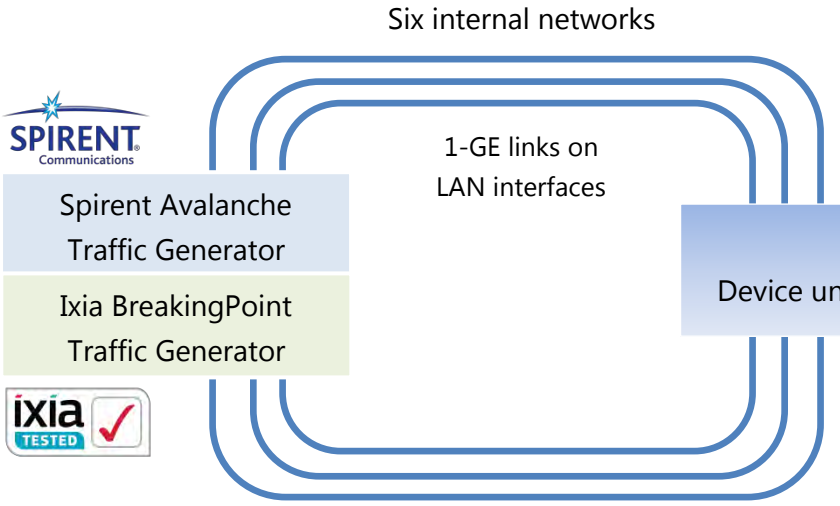
Throughput is just one useful metric when implementing network security appliances in a business environment; security is equally important. But network performance impact helps IT departments make a practical choice between similar, highly secure network appliances.

Test Tools

Source: Miercom July 2017

The test tools featured above are used for real-time traffic generation, traffic monitoring and data capture throughout testing.

Test Bed Diagram



- UDP (1518-byte and IMIX)
- 50 simulated users per interface with 100 HTTP/HTTPS GET requests per user, retrieving the same 1 MB .dat (binary) file

Source: Miercom July 2017

Traffic was sent to each DUT through three LAN ports and responses were received through three other LAN ports, for a total of six interfaces. The Spirent Avalanche generated external client traffic on three 1-GE links to the security appliance under test and issued internal server responses on three 1-GE interfaces. Traffic represented a real-world, high-stress network scenario of client-server connections supporting both stateless UDP and stateful HTTP and HTTPS traffic.

For initial baseline tests, stateless UDP and stateful HTTP and HTTPS traffic were used.

For stateless traffic, 250 bidirectional discrete flows of UDP packets were sent on all six 1-GbE interfaces, delivering a total of 6 Gbps to and through the DUT. This was sent in two loads for two separate tests:

1. UDP with all large, 1518-byte packets
2. UDP with IMIX of 48-byte (60.7 percent), 576-byte (23.7 percent) and 1500-byte (15.7 percent) packets for a total of 10,000 packets

Throughput for each DUT was observed for the maximum rate in megabits per seconds (Mbps) before a single packet was lost. Results are featured in Chart 1 (page 10).

For stateful traffic, there were 50 users on the client side sending an HTTP GET request to download 1 MB binary .dat file from 50 simulated servers. There were 100 GET requests per user on the client side. This procedure was followed for both:

1. HTTP
2. HTTPS using AES256 and SHA256 encrypted packets

Throughput was observed for its maximum rate in Mbps before any transaction of file transfer failed. This testing was repeated for each DUT with additional individual security services enabled and with full UTM mode. Performance was compared to the baseline throughput to determine the effect the security service has on each DUT.

Stateful throughput using HTTPS was tested with decryption capabilities enabled. However, the Sophos XG 210 and Fortinet FortiGate 100E HTTPS encryption and decryption required enablement of at least one security feature. In Sophos' case, any configuration with decryption required that AV was also enabled; Fortinet required at least one other security service. Therefore, HTTPS baselines for Sophos and Fortinet were not available. Additionally, the performance of HTTPS with IPS only enabled for Sophos was not available, as it would automatically require AV enablement. These items were not included in Chart 2 (page 12) and Chart 3 (page 13) to maintain fair comparisons.

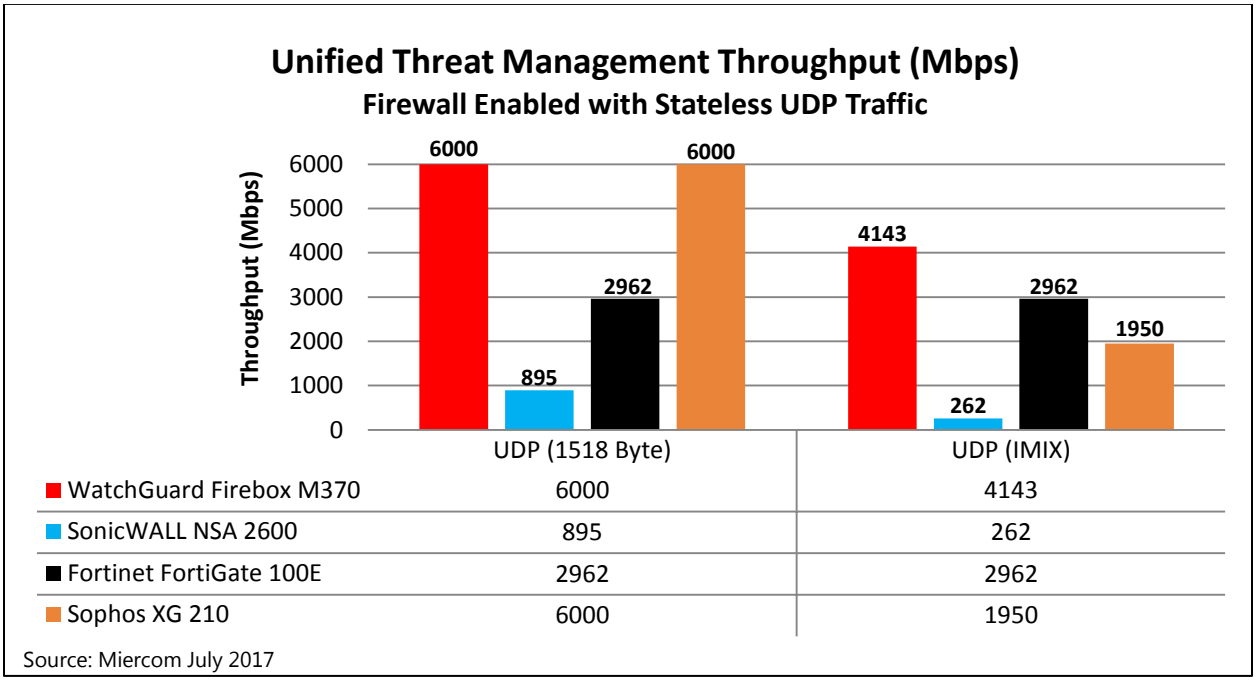
Performance Testing

Stateless UDP 1518-Byte and UDP IMIX Throughput

This test measured the maximum rate of traffic of the security appliance under test in Mbps. Only the firewall security service was enabled since it is the most basic and fundamental service of a security appliance.

For the first test, stateless bidirectional UDP 1518-byte packets were sent on all six interfaces for a maximum of 6 Gbps of traffic. Then the second stateless traffic test used bidirectional UDP IMIX traffic, wherein the packet size varied using the following distribution: 60.7 percent small packets (48-byte), 23.7 percent mid-sized packets (576-byte), and 15.7 percent large packets (1500-bytes).

Chart 1: Unified Threat Management Throughput for Stateless UDP Traffic



Source: Miercom July 2017

The WatchGuard Firebox M370 achieved the maximum throughput performance of 6 Gbps for UDP traffic using uniform 1518-byte packets. This performance was matched only by the Sophos XG 210. WatchGuard's performance was 85 percent higher than SonicWALL and 51 percent better than Fortinet. When measuring performance for the more realistic UDP IMIX packets, WatchGuard had the highest throughput at 4.1 Gbps, which was 94 percent higher than SonicWALL, 29 percent better than Fortinet and 53 percent higher than Sophos. With the exception of Fortinet, where no degradation in performance was observed for uniform and IMIX UDP traffic, WatchGuard displayed the lowest loss in performance, with only a 30 percent loss. SonicWALL showed 71 percent loss and Sophos had 68 percent loss.

Stateful Throughput (HTTP/HTTPS)

Most Internet traffic uses the stateful Layer-7 application protocol HTTP to establish client-server connections over Layer-4 Transmission Control Protocol (TCP). Networks can upload and download files from the public Internet using HTTP, requiring high-level processing and inspection for malicious content.

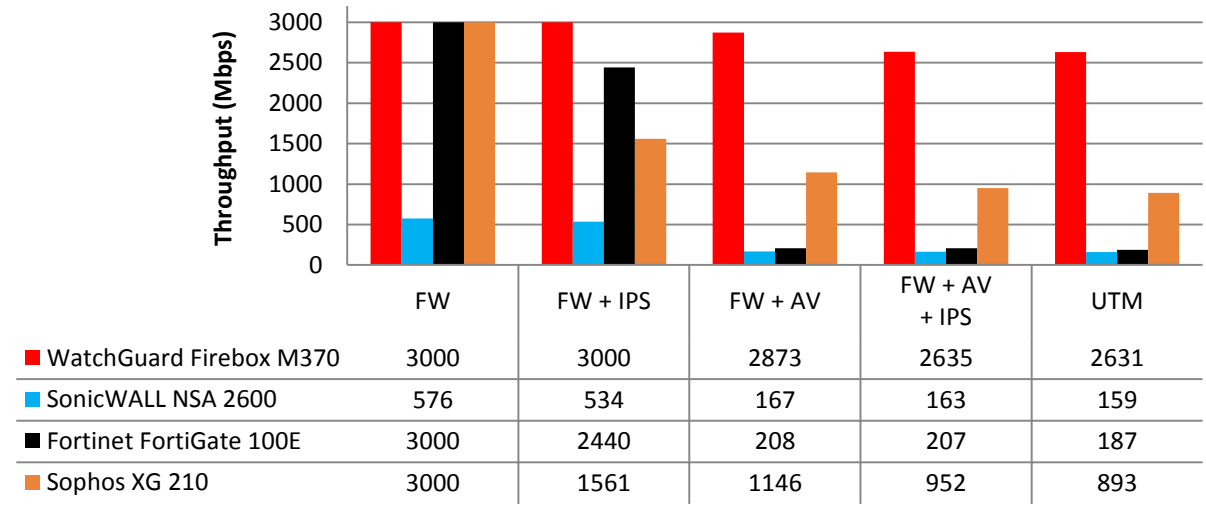
The most basic inspection is done using a firewall, with additional security services available from vendor to vendor. The most popular services include: decryption, IPS, AV and application control. The test results below reflect similar security appliances with firewall and decryption enabled as a baseline, and additional security features applied using the following configurations:

1. **FW (Baseline).** Only the firewall was enabled to HTTP traffic stream.
2. **FW + IPS.** IPS was enabled, in addition to the firewall.
3. **FW + AV.** Web/HTTP proxy and AV processing was enabled, in addition to the firewall. Prior to the performance testing of this configuration scenario, a special test virus look-alike, called EICAR, was included in the files sent to ensure the appliance's antivirus processing was appropriately configured, scanning files and flagging viruses.
4. **FW + AV + IPS.** AV and IPS were enabled, in addition to the firewall.
5. **Full UTM.** Where the appliance's AV, IPS and Application Control were all concurrently enabled and applied, in addition to the firewall.

The Spirent Avalanche generated increasing loads of HTTP test traffic over three pairs of interface where 50 simulated clients per interface launched 100 GET requests to 50 simulated servers, resulting in a download retrieval of 1 MB binary file. Client and server sides were separated by different LANs.

Similarly, stateful HTTPS traffic loads were sent through the DUT using the configuration and test setup. The AES256 and SHA256 encryption standards were used to secure traffic on the application layer with HTTPS. When the 1 MB binary file was requested, each packet was decrypted and re-encrypted before transfer. This processing was expected to place a load on the security appliance and throughput. The importance of encrypted traffic is to combat security threats, but attackers commonly use this very countermeasure to obfuscate malware until it reaches its destination. Each DUT should be capable of examining encrypted messages without severely degrading its throughput.

Chart 2: Unified Threat Management Throughput for Stateful HTTP Traffic

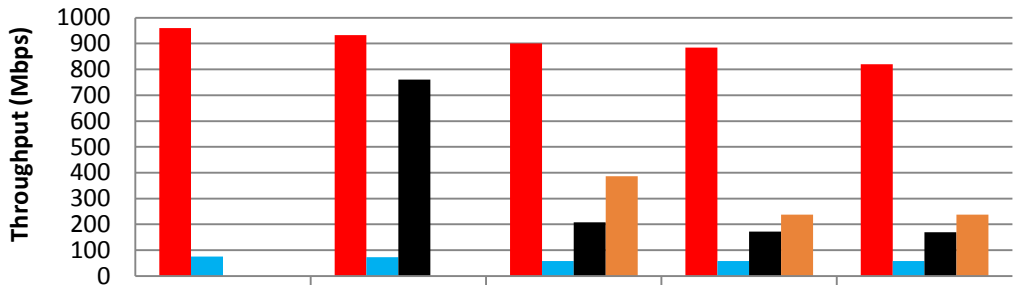


	FW	FW + IPS	FW + AV	FW + AV + IPS	UTM
WatchGuard Firebox M370	3000	3000	2873	2635	2631
SonicWALL NSA 2600	576	534	167	163	159
Fortinet FortiGate 100E	3000	2440	208	207	187
Sophos XG 210	3000	1561	1146	952	893

Source: Miercom July 2017

WatchGuard, Fortinet and Sophos all had the highest throughput for its HTTP baseline at 3 Gbps. But unlike its competitors, WatchGuard had no degradation when the IPS service was enabled, maintaining 3 Gbps throughput and performing at least 19 percent higher than its closest competitor. WatchGuard continued to have higher throughput than competing devices for AV enabled, AV and IPS enabled, and full UTM mode. When comparing full security service performance to its baseline, WatchGuard was reported having only 12 percent degradation of performance, while Sophos saw 70 percent loss and Fortinet's rate fell by 94 percent. WatchGuard had the highest UTM throughput, three times the throughput of its closest competitor. Enabling security features on the WatchGuard Firebox M370 had less degradation on its performance over HTTP than similarly tested products.

Chart 3: Unified Threat Management Throughput for Stateful HTTPS Traffic



	FW	FW + IPS	FW + AV	FW + AV + IPS	UTM
WatchGuard Firebox M370	960	933	901	885	820
SonicWALL NSA 2600	75	73	58	58	58
Fortinet FortiGate 100E	N/A	760	208	172	169
Sophos XG 210	N/A	N/A	387	238	238

Source: Miercom July 2017

Fortinet and Sophos were not available for baseline comparison since HTTPS inspection required at least one additional security service to be enabled. WatchGuard outperformed SonicWALL by 92 percent for the firewall over HTTPS. Despite SonicWALL's lower throughput, it saw little degradation as security services were applied, losing only 23 percent of its throughput from baseline to full UTM mode. SonicWALL and Fortinet had more of a performance impact from AV than IPS, while WatchGuard outperformed its closest competitor by 71 percent. In full UTM mode for HTTPS traffic, WatchGuard had the highest throughput at 820 Mbps. Inspecting encrypted traffic had an impact on every vendors' performance, but WatchGuard maintained the highest throughput of its competitors for all tests.

The Fortinet FortiGate 100E and Sophos XG 210 products did not have comparable baselines since firewall could not be enabled alone with HTTPS traffic. Fortinet required either AV or IPS service. In the case of Sophos, decryption required AV to be enabled, such that the FW + IPS test result could not be accurately reported and was not available for comparison.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed. Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

Customer Use and Evaluation

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every possible deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform an on-site evaluation.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.