Unified Threat Management
Comparative Throughput Performance

WatchGuard Firebox T70

Fortinet FWF-92D

SonicWALL TZ600

Sophos SG135W

DR160930C
October 2016

Miercom
www.miercom.com

Contents

Executive Summary

Miercom was engaged by WatchGuard Technologies, Inc. to conduct independent, comparative throughput performance testing of four market-leading Unified Threat Management (UTM) network-security appliances: from WatchGuard, Fortinet, SonicWALL and Sophos.

This report details the results and load impact on network performance in the following scenarios:

- **Baseline performance.** Network-layer throughput with firewall filtering enabled; this was measured using large, 1518-byte packets and then an IMIX assortment of varied packet sizes. Baselines were taken for UDP (user datagram protocol) and TCP (transmission control protocol)-based HTTP, as well as encrypted HTTPS (HTTP Secure).
- **Firewall with other security features enabled.** Features and functions in addition to firewall were then individually enabled to evaluate how these impacted performance.
- **Full UTM mode**. Throughput with the full set of security functions enabled and running (firewall, intrusion prevention system, antivirus and application control) was then tested.

Key Findings

- WatchGuard exhibited the best multi-function and full-UTM performance, consistently processing over 1 Gbps of HTTP throughput. The next best HTTP performer, Dell's SonicWALL, delivered just 64 percent of WatchGuard's full-UTM throughput.
- WatchGuard also delivered the best throughput performance for encrypted HTTPS traffic, which is a major source of malware infection. In fact, WatchGuard's HTTPS throughput was more than double the nearest competitors' in all scenarios.

Overall, the WatchGuard Firebox T70 exhibited by far the best throughput performance of the competitive security appliances tested. In addition, while competitors' performance tanked as more security functions and features were enabled, the WatchGuard Firebox T70's did not.

Based on the results of this testing, the WatchGuard Firebox T70 exhibits exceptional throughput when running multiple functions and full-UTM, and we proudly award it the Miercom Performance Verified certification.

Robert Smithers
CEO
Miercom

Introduction

Unified Threat Management

Unified Threat Management devices are the latest, and 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, at a minimum, the same set of five security functions. Key security features typically found in UTM products are discussed more 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.
HTTP (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.
HTTPS (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: firewalling, IPS, AV, VPN (control of virtual private network tunnels), content filtering, and sensitive data loss prevention.

UTM devices contain and perform much the same combination of security functionality as Next-Generation Firewalls and Secure Web Gateway devices. UTM products, however, are typically designed for small and mid-sized businesses. When considering a UTM device, a balance between network performance and security must be considered. As the amount and effectiveness of security processing increases, throughput performance inevitably slows.

In this and other testing of UTMs, throughput baselines are first obtained. As discussed later, only basic "firewall" functionality is enabled in baseline testing. With some devices the basic firewall inspection of traffic cannot be disabled.

As firewall scanning performs fairly low-level, typically just network-layer, scanning of passing traffic, baseline testing represents the most throughput that can be achieved for a given UTM device. Comparing the baseline rate with the throughput when other security features are incrementally added shows how throughput decreases as the additional processes are enabled.

Throughput performance is just one useful metric when implementing network security. The efficacy of the security appliance – its ability to catch most of all of the malicious threats of all sorts – is another, obviously important one.

Products Tested

Vendor / UTM Product	Software/firmware Version
WatchGuard / Firebox T70	11.11.3
Dell SonicWALL / TZ600	6.2.6.0-20N
Fortinet / FWF-92D	5.4.0
Sophos SG 135w	9.405-5*

* This version of Sophos firmware, 9.405-5, is an older but widely deployed Sophos version in customer sites. Testing was also conducted with a later version 15 firmware and, where differences occurred, the better average throughput is shown in the results here.

WatchGuard

The *Firebox T70* is the latest and most powerful offering in WatchGuard's Firebox series. It, too, is oriented towards small businesses. Features supported include: firewall, VPN, IPS, application proxies for various protocols (HTTPS, HTTPS, SMTP, DNS and others) and reputation-based antivirus (reputation-based means a context assessment of suspicious files based on their location, frequency and other characteristics). Routing is policy based, and reporting is simple. This WatchGuard appliance implements the Intel AES-NI instruction set for fast encryption processing.

The Firebox T70 features eight gigabit Ethernet copper interfaces, including two supporting PoE and supports up to 800,000 concurrent bi-directional connections.

Dell SonicWALL

The *Dell SonicWALL TZ600* is intended for distributed enterprises and remote offices, managed by a central office. It incorporates firewall, VPN (IPSec and SSL-based), IPS, and application control using proprietary deep packet inspection and policy-based filtering over both secure and unsecure connections.

The SonicWALL TZ600 supports eight configurable gigabit Ethernet copper ports, plus LAN and WAN ports, and can reportedly apply DPI (deep packet inspection) on up to 125,000 connections.

Fortinet

The *Fortinet FortiGate 92D* is called a Next Generation FireWall (NGFW) UTM appliance bundle. The product protects distributed network locations via a central unified policy management system. The device incorporates firewall, IPS, VPN (IPsec and SSL based), and can apply various filtering controls on network traffic.

The FortiGate 92D features 16 Gigabit Ethernet copper interfaces, 16 GB of memory, and high-availability configurations.

Sophos

The *Sophos SG 135w* is an appliance designed for use by small and medium enterprises looking for a device that provides consolidated firewall, VPN, IPS and AV-proxy functionality. It features Intel multi-core processors providing considerable processing power. All Sophos SG devices support high availability configuration and can be centrally managed through Sophos Firewall Manager. This UTM allows additional functionality to be added as needed through software upgrades, without requiring additional hardware.

The SG-135w features 6 GB RAM, 64 GB of solid-state storage and eight Gigabit Ethernet copper interfaces. The appliance supports up to 2 million concurrent connections.

How We Did It

Measuring the impact of security functions on network throughput performance was the main objective of our test methodology. Miercom simulated a robust and realistic testing environment to determine the performance of each security appliance under different configuration scenarios. Devices were configured for optimal throughput, while the security features were deployed.

Initially, a series of baseline tests were run, measuring throughput of each competitive device with only its base firewall running. Traffic was run bi-directionally over four 1-Gbps copper interfaces at full load – a maximum possible total load delivered to each appliance of 4 Gbps.

The baseline measurements are throughput of just the firewall without any other security features enabled. The baseline traffic was applied in different loads:

1. **UDP flows**: 250 flows each consisted of all 1518-byte packets. The IP addresses were incremented by 1 in the last octet and the MAC addresses were stepped up in the third octet. All packets were connectionless UDP (user datagram protocol) and UDP port numbers started at 1753 and incremented by 1 for each client.
2. **IMIX load**: The same as the UDP load, except packet lengths were varied using a test mix called IMIX, which better represents real-world Internet traffic. With this mix, packets are sent with this distribution: 60.6 percent are small, 48-byte packets; 23.6 percent are mid-sized, 576-byte packets; and 15.6 percent are large, 1500-byte packets.

Baseline tests were also run with stateful HTTP traffic, and then with stateful, encrypted HTTPS traffic. Firewall processing does not typically get involved with the higher-layer, stateful nature or application of traffic. But even so, the baseline test results for HTTP were considerably lower than the UDP or IMIX throughputs. The HTTPS baseline throughput is seriously diminished in most cases by the processing required to decrypt and then re-encrypt the passing traffic.

Then, after baselining, each additional security feature (see below) was enabled and tested – in addition to the firewall – to demonstrate its effect on the overall network throughput performance. The final test of the series was the UTM security configuration, which included firewall, IPS, application control, and antivirus features.

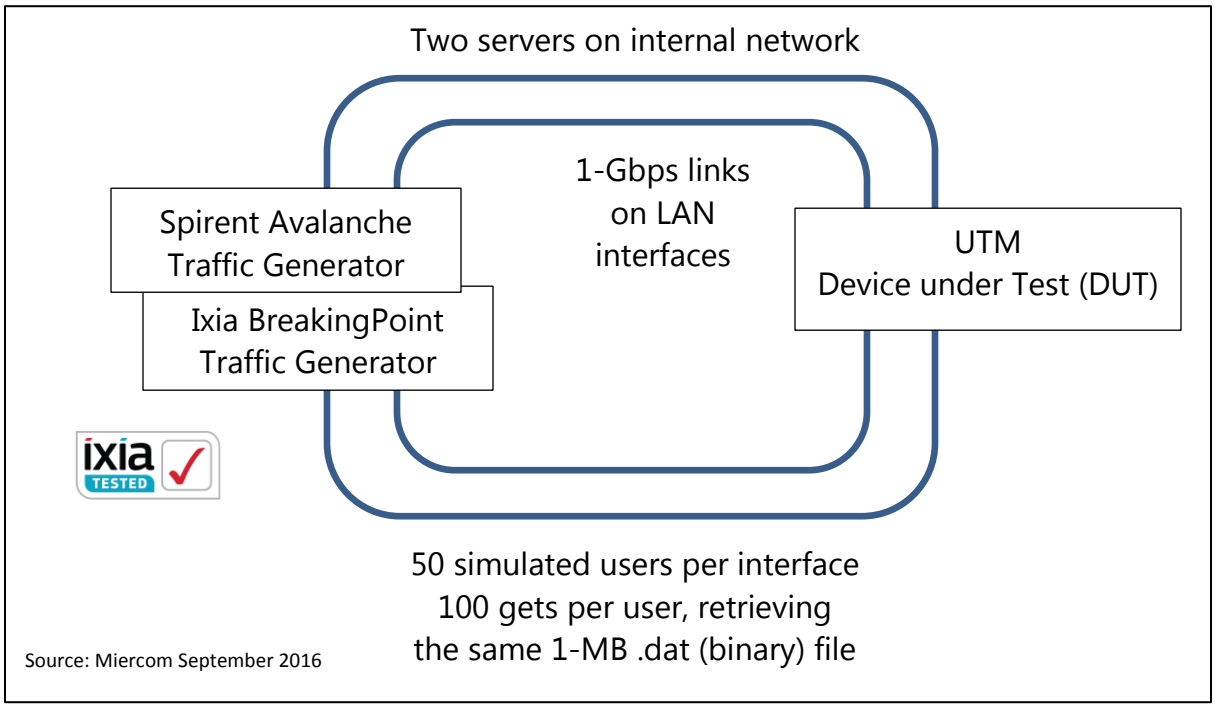
- Firewall + IPS
- Firewall + HTTP Proxy/Antivirus
- Firewall + HTTP Proxy/Antivirus + IPS
- Full UTM: Firewall + IPS + Proxy/Antivirus + Application Control, all applied concurrently

The testing, then, focused on the loading effect that additional security function places on the throughput performance of the network.

Test Bed Setup

Traffic was sent to each security device through LAN ports and responses received back through two other LAN ports. A Spirent Avalanche test-traffic generator issued "client" traffic on two 1-GE (Gigabit Ethernet) links to the security appliance under test, and issued "server" responses on two other 1-GE interfaces, as shown in the test-bed diagram below.

UTM Test Bed



As the diagram shows, *Spirent Avalanche* clients were external and connected to two LAN ports of the Device under Test (DUT). *Avalanche* servers were on the protected internal network and likewise connected through LAN ports of the DUT.

The *Spirent Avalanche* generated traffic for each DUT. The traffic represented a real-world, high-stress network scenario of client-server connections supporting both stateless User Datagram Protocol (UDP) and stateful HTTP and HTTPS traffic.

For initial baseline tests, stateless UDP traffic consisting of 250 discrete flows was sent on all four 1-GE interfaces, delivering a total of 4 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 packets (60.7 percent), 576-byte (23.6 percent) and 1500-byte (15.7 percent)

Throughput Tests

Baseline UDP

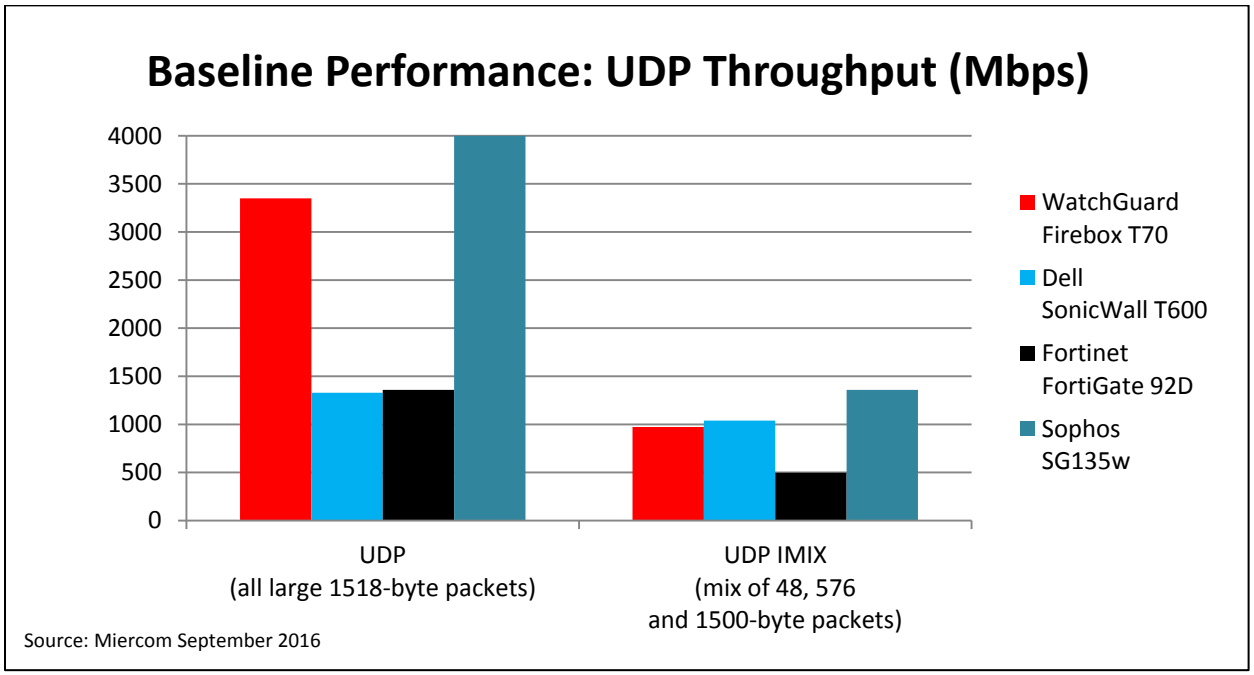
Description

This baseline throughput test measured the maximum rate of traffic successfully processed by the security appliance under test, in mbps. These tests were performed with only the firewall function enabled. In the first test round, stateless UDP traffic consisting of all 1518-byte packets was sent on all four interfaces, comprising 4 Gbps of throughput.

In the second test round, stateless UDP traffic was again sent, except packet size varied with the IMIX distribution: 60.7 percent small packets (48 byte), 23.6 percent mid-sized packets (576 byte), and 15.7 percent large packets (1500 bytes).

Results

The chart below displays maximum achievable throughput rates for each appliance. The Spirent Avalanche meticulously compares the packet rate of received data with the packet load sent. Sending all large packets tends to maximize throughput. However, this is unrealistic in the real world. The second set of UDP tests used the IMIX packet-size distribution, which sends many more packets per second, since most are small (just 48 bytes). Processing packets requires overhead which affects even network devices like switches and routers, and it tends to significantly reduce throughput.



WatchGuard delivered over 80% of its load, while Dell and Fortinet processed only around one-third. The IMIX distribution of UDP packet sizes reduces throughput performance considerably. Sophos achieved about 1.3 Gbps. WatchGuard and Dell SonicWALL achieved a little less at about 1 Gbps, and Fortinet could process only around 500 Mbps.

HTTP Throughput

Description

The vast majority of Internet traffic today – some say over 80 percent – is Web file retrievals, which are transported via the Hypertext Transmission Protocol, or HTTP. This is a stateful protocol that establishes connections between clients and servers over the Layer-4 Transmission Control Protocol (TCP).

The primary use of HTTP is to get files over the Internet, whether Web pages or downloaded files. In our testing the Spirent Avalanche generated high volumes of HTTP test traffic over two pairs of interfaces. Fifty client users per interface each launched 100 gets to a server, each resulting in the download retrieval of a 1-MB binary file.

The same HTTP test traffic was delivered in five different test scenarios

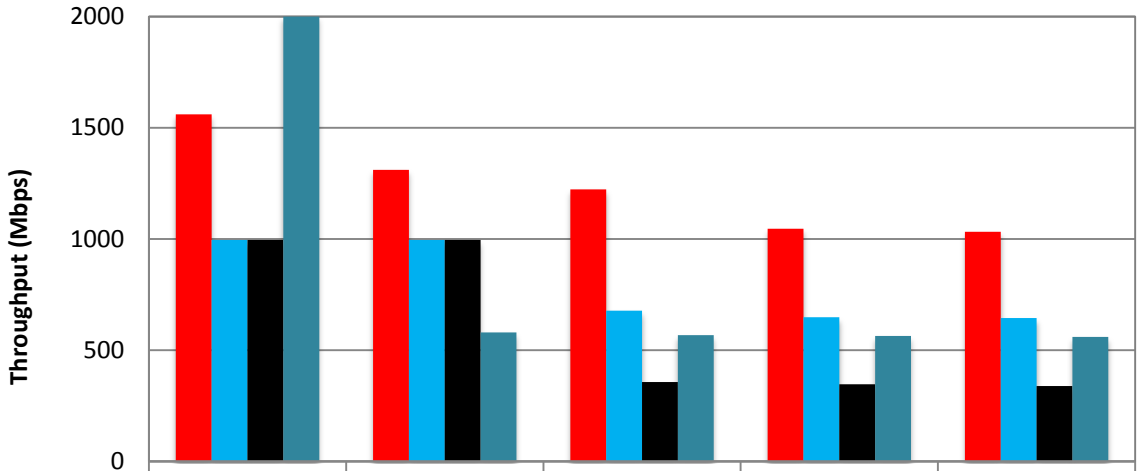
1. Firewall Baseline: Where only the appliance's firewall was applied to the HTTP stream.
2. Firewall + IPS: Where the appliance's Intrusion Prevention System (IPS) was enabled and applied, in addition to the firewall.
3. Firewall + AV: Where the appliance's Web/HTTP proxy and Antivirus (AV) processing was enabled and applied, 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 and that it was indeed scanning files and doing its job. In all cases the EICAR test virus was identified and flagged.
4. Firewall + AV + IPS: Where the appliance's Antivirus and IPS were enabled and applied, in addition to the firewall.
5. Full UTM: Where the appliance's Antivirus, IPS and Application Control were all concurrently enabled and applied, in addition to the firewall.

In all cases multiple test runs were conducted. In a few cases there was variability in the results, so the results of the multiple runs were averaged to yield the results shown in the following chart.

Results

The HTTP throughput results, shown in the chart on the next page, reveal the variability between security appliances as more and more security functions are enabled.

HTTP Throughput Performance (Mbps)



	Firewall (Baseline)	Firewall + IPS	Firewall + AV	Firewall + AV + IPS	Full UTM (FW + AV +IPS + AppCtrl)
WatchGuard Firebox T70	1560	1311	1223	1046	1032
Dell SonicWall TZ600	996	996	678	648	645
Fortinet FortiGate 92D	996	996	357	347	339
Sophos SG135w	2000	580	568	564	560

Source: Miercom September 2016

For HTTP processing, WatchGuard had a baseline throughput of over 1.5 Gigabits/second. Baseline throughput of Dell and Fortinet were about 1 Gbps of HTTP traffic and neither were impacted by also enabling their IPS. Sophos' throughput dropped from 2 Gbps to 580 Gbps with IPS enabled, whereas WatchGuard only fell slightly from 1.5 Gbps to 1.3 Gbps when IPS was applied. The addition of AV had the biggest effect on Fortinet, reducing its baseline throughput by two-thirds, to 350 Mbps. WatchGuard and Sophos only saw a small drop, close to their IPS throughput. With full UTM, only WatchGuard could still deliver over 1 Gbps of HTTP throughput, representing 40 percent more than Dell's, nearly double Sophos', and three times Fortinet's throughput.

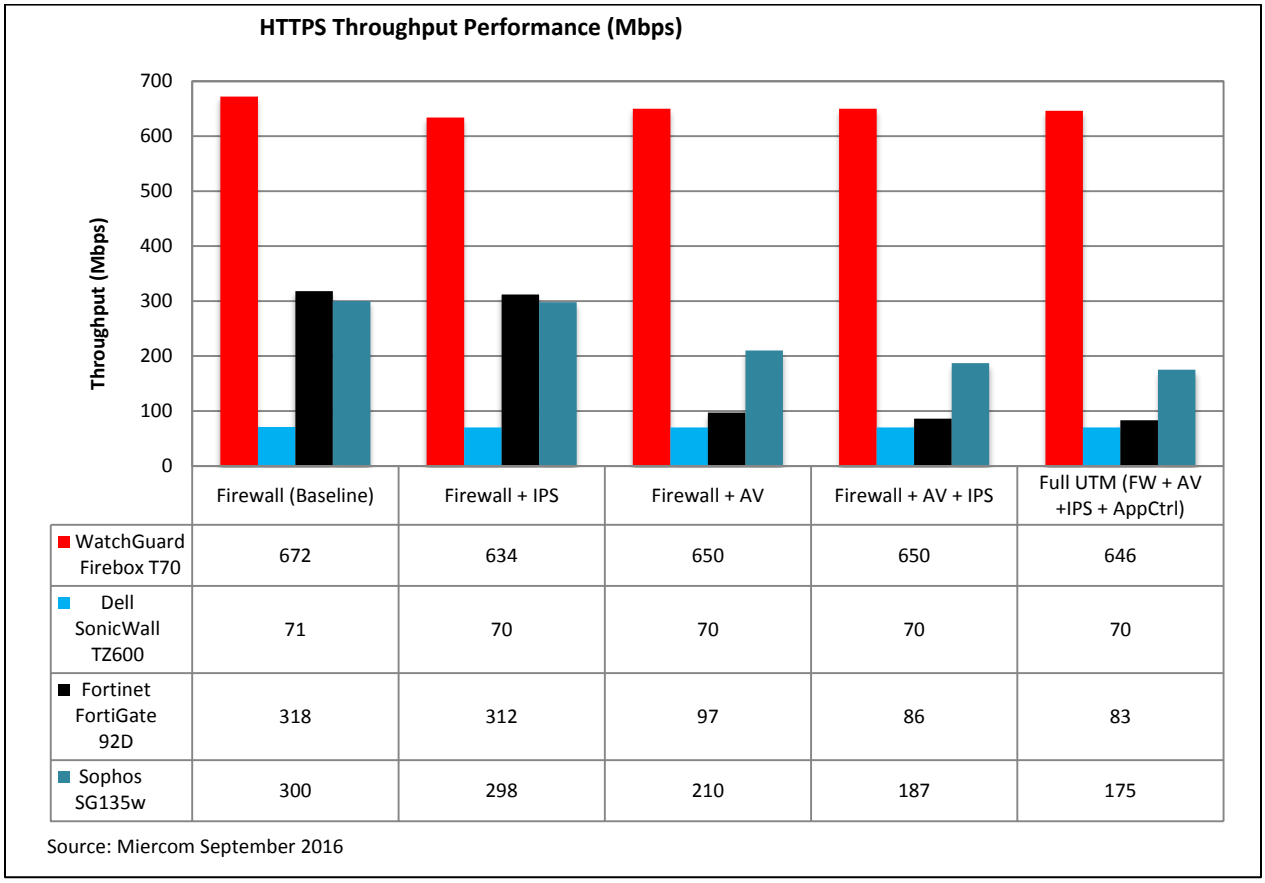
HTTPS Throughput

Description

The major difference between HTTP and HTTPS is the encryption of packet content above the transport layer. Each pack is decrypted and reencypted before transfer, placing a load on the appliance. Our test team checked to ensure that each security appliance did indeed process packets in this fashion and measured HTTPS performance.

Internet traffic is increasingly using the HTTPS protocol, amid heightened security concerns. However, since HTTPS typically remains encrypted until received at the destination computer, it has also become a vector for delivery of viruses and malware. For this reason, users are keen to deploy security equipment – UTMs –capable of examining encrypted messages and packets. However, there is a throughput performance price to pay.

Results



	Firewall (Baseline)	Firewall + IPS	Firewall + AV	Firewall + AV + IPS	Full UTM (FW + AV +IPS + AppCtrl)
WatchGuard Firebox T70	672	634	650	650	646
Dell SonicWall TZ600	71	70	70	70	70
Fortinet FortiGate 92D	318	312	97	86	83
Sophos SG135w	300	298	210	187	175

Source: Miercom September 2016

WatchGuard had remarkable HTTPS throughput performance, showing a processing rate well over 600 Mbps of encrypted traffic. And while this rate was only half of its HTTP performance, it was considerably more than any of its competitors'. WatchGuard's IPS-enabled performance was more than double Fortinet's and Sophos', and almost ten times Dell's throughput. Dell's degraded baseline performance indicated an extraordinary load incurred by handling decryption/encryption. Fortinet saw the most impact when enabling AV, dropping 75 percent to about 85 Mbps. Sophos similarly was affected by encryption processing; its throughput was less than half its non-encrypted counterpart for the same scenarios.

Conclusions

This testing revealed some remarkable achievements by WatchGuard with its new Firebox T70, in all mixed-function scenarios and encryption processing, compared to the competitive security appliances tested.

WatchGuard's Firebox T70 delivered more than 1 Gigabit/sec of HTTP throughput in every scenario: firewall, and with IPS, Antivirus and Application Control running along with firewall, in any combination.

In Full-UTM mode, with all tested security functions running concurrently, WatchGuard achieved 1.032 Gbps of HTTP throughput. This represents:

- 38 percent more than the Dell SonicWALL TZ600
- 46 percent more than the Sophos SG 135w
- 68 percent more than the Fortinet FortiGate 92D

In Full-UTM mode, with all tested security functions running concurrently, WatchGuard achieved 646 Mbps of encrypted HTTPS throughput. This represents:

- Over 9 times more than the Dell SonicWALL TZ600
- Over 3.6 times more than the Sophos SG 135w
- Over 7.7 times more than the Fortinet FortiGate 92D

Independent Evaluation

This report was sponsored by WatchGuard Technologies, Inc. The test results were validated completely and independently as part of Miercom's competitive analysis of these UTM products.

About Miercom

Miercom has published hundreds of network-product-comparison analyses – many made public, appearing in leading trade periodicals and other publications, and many confidential, for internal use only. 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 test methodologies are generally developed collaboratively with the client, and feature 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.

Use of This Report

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

This document is provided "as is" by Miercom, which 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 herein. Miercom is not liable for damages arising out of or related to the information contained in this report.