



Unified Threat Management
Throughput Performance
Rackmount Device Comparison

SOPHOS

DR150819C
October 2015

Contents

Executive Summary	3
Introduction	4
Products Tested	6
How We Did It.....	7
Throughput Test.....	9
Firewall	10
Firewall and Intrusion Prevention System	11
Firewall and Application Control.....	12
Firewall and HTTP Proxy/Antivirus.....	13
Firewall and HTTPS.....	14
Unified Threat Management.....	15
Conclusion	16
Fair Test Notification.....	17
About Miercom.....	17
Use of This Report	17

Executive Summary

Miercom was engaged by Sophos to conduct independent performance testing of the Sophos SG135w unified threat management (UTM) desktop firewall device as a network security solution. The SG135w was compared to rackmount devices, showing that this UTM can be viable alternative to the larger rack mount devices. Testing, which employed industry-leading performance testing equipment, was conducted in July 2015.

Throughput performance measurements were recorded on the firewall only and then subsequently with various traffic loads applied. Firewall throughput without any other functions enabled is referred to as the baseline in this report. Tests were then performed with another function (e.g. intrusion prevention system), enabled on the firewall. Finally, the full UTM mode, all the functions were combined and run. These results were compared to competing vendors and the baseline firewall rate. All results shown in this report were based on actual observations in our laboratory.

Key Findings

- Baseline firewall throughput was the highest at 5400 Mbps, 51% better than the rackmount vendor average
- Higher throughput was obtained for firewall deployed with intrusion prevention system, application control, HTTP Proxy/Antivirus, HTTPS than other vendors
- Highest throughput for secured network communication, at 1020 Mbps; over 26% above the vendor average rate for processing classified traffic

The Sophos SG135w performed better than the vendor average, and its UTM traffic handling capability was among the highest on the market, proving the desktop device has comparable capabilities to rack mount devices.

Based on the results of our testing, we proudly award the Miercom Performance Verified Certification to the Sophos SG135w.

Robert Smithers
CEO
Miercom



Introduction

Unified Threat Management

Unified Threat Management (UTM) devices are a class of network edge security platforms that address multiple security functions in a single chassis.

The baseline is throughput of the firewall without any other features enabled. Each feature described below was enabled and tested with the firewall to demonstrate its effect on the firewall performance. The unified security configuration which included firewall, IPS, application control, and antivirus features were applied as the final test of the throughput performance.

Some of the features typically found in a UTM device are described below.

Feature	Acronym	Description
Firewall	FW	<i>Controls and filters flow of traffic within a network with a barrier to protect trusted internal network from an unsecure network (e.g. Internet)</i>
Intrusion Prevention System	IPS	<i>Monitors network and system activity for malicious behavior based on signatures, statistical anomalies, or stateful protocol analysis. If malicious packets are detected, they are identified, logged, reported, and attempted to be blocked access to the network.</i>
Application Control	AppCtrl	<i>Enforces policies regarding security and resources by restricting/controlling which applications can traverse through the UTM. It intends to reduce occurrences of infection, attacks, and negative consequences of malicious content.</i>
Hypertext Transfer Protocol Proxy/Antivirus	HTTP Proxy/AV	<i>A client issues a request which is sent to the proxy to buffer the file in memory. The file is then sent to an antivirus engine to for viruses, removing packets which contain malicious content. Proxy-based scanning is a more secure and accurate method, in comparison to a stream-based antivirus inspecting traffic between the client and server. Proxy/AV performs scanning during the handshake of data transfer.</i>
Hypertext Transfer Protocol Secure	HTTPS	<i>Responds to incoming encrypted connection requests on the secure socket layer (SSL) while actively blocking other packets containing malicious content. This differs from HTTP requests in that the encryption/decryption process places a load on the device and directly affects its throughput rate.</i>
Unified Threat Management	UTM	<i>All-inclusive security with multiple functions in central unit. Contains firewalling, IPS, AV, VPN, content filtering, and sensitive data loss prevention.</i>

UTM devices contain the same functionality as Next-Generation Firewall and Secure Web Gateway devices, Secure Email Gateways, and Wireless controllers performing multiple security

features in one system. UTM products are designed for small and mid-sized businesses. When considering a UTM device, a balance between network performance and security must be considered. Adding security will slow throughput performance.

UTM's were tested in order to show what effect the implementation of additional security features had on the throughput.

Comparing the baseline rate with the throughput when features were added provided metrics showing the decreased throughput as additional processes were enabled. These tests were run on the rackmount models and compared.

Throughput performance is one metric needed when implementing network security. Performance degradation needs to be minimal in enterprise networks.

Products Tested

Name	Version
Sophos SG135w	9.313-3
Dell SonicWall NSA 2600	SonicOS Enhanced 6.1.2.3-20n
Fortinet FortiGate100D	v5.2.3, build670
WatchGuard XTM 525	11.10.1.B477570

Sophos

The *Sophos SG 135w* is for small enterprises looking for flexible, high-speed devices that provide firewall, VPN, IPS and AV-proxy for their network. It features multicore processors providing ample processing power for the security features enabled. The SG135w can have up to 10 clustered units and be managed through the Sophos UTM Manager (SUM). This UTM allows protection to be added as needed, through software upgrades, without additional hardware.

Dell

The *Dell SonicWall NSA 2600* is a comprehensive product for local and remote connections for branch offices. By aggregating firewalls, IPS with deep packet inspection, antivirus, and application control, this device deflects current and zero-day threats attempting to breach a network.

Fortinet

The Fortinet *FortiGate 100D* prevents threats from entering medium sized enterprises or remote branches with one management console, capable of multiple technologies for detecting attacks; they consist of firewall, VPN, application control, IPS, antivirus, and web filtering.

WatchGuard

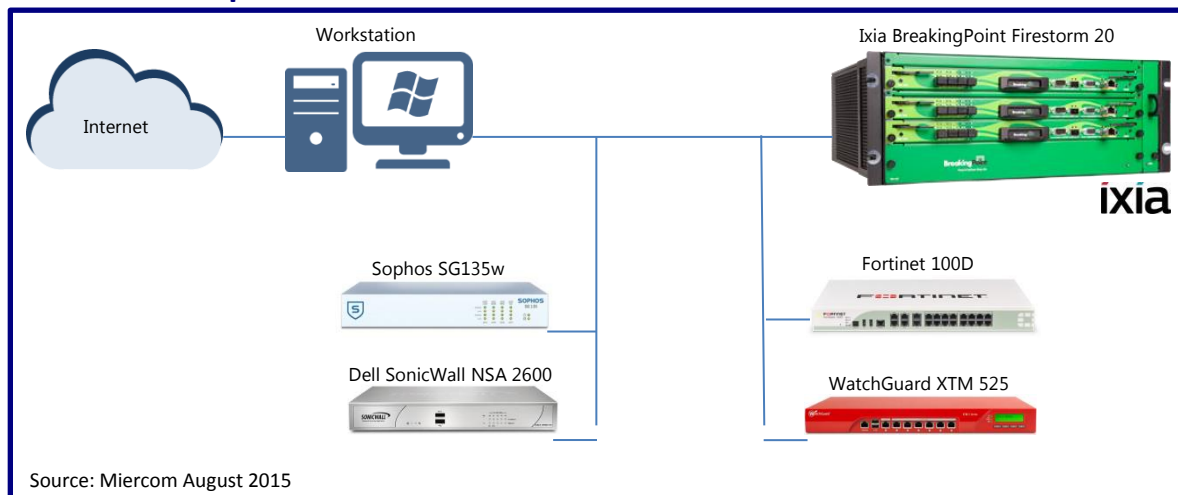
The *WatchGuard XTM 525* delivers all-in-one protection for medium sized businesses. Services include firewall, VPN, IPS, application control and antivirus with full secured traffic, deep packet inspection. The XTM 525 has low power usage.

How We Did It

The impact of security on network performance is a key component of this test methodology. Miercom used an industry leading test tool to provide a robust and realistic testing environment. Appliances under test were configured for optimal functionality to enable maximum throughput, while the security features were deployed.

Testing focused on the loading effect that additional security functions place on the performance of the network.

Test Bed Setup



The *Ixia BreakingPoint FireStorm 20* generated traffic for each device under test. This product creates real-world traffic to simulate high-stress network conditions where security devices may be evaluated for their performance under loads of greater application inspection functionality than basic firewalls.

FireStorm 20 functionality includes:

- Application control that can stress and overload Deep Packet Inspection (DPI) devices
- Client-side SSL bulk encryption – performed at up to 25 Gbps without a cipher
- The ability to measure network latency down to a 10-nanosecond granularity

The FireStorm20 allows organizations to:

- Reduce time-to-test to minimize costs and accelerate development of next-generation network, security and data center devices
- Cost-effectively perform complex, real-world simulations in order to evaluate, test and optimize application-aware devices
- Train and certify IT personnel to predict and prevent cyber-attacks

Traffic Generation

The *Ixia BreakingPoint Firestorm 20* generated traffic for each device under test. The traffic represented a real-world network scenario of client to server connections using high-density ports supporting stateful traffic. BreakingPoint can simulate over 200 applications and more than 35,000 live security attacks. The Firestorm performs complex simulations to test throughput of network security appliances.

Traffic was sent with these protocols for the following tests:

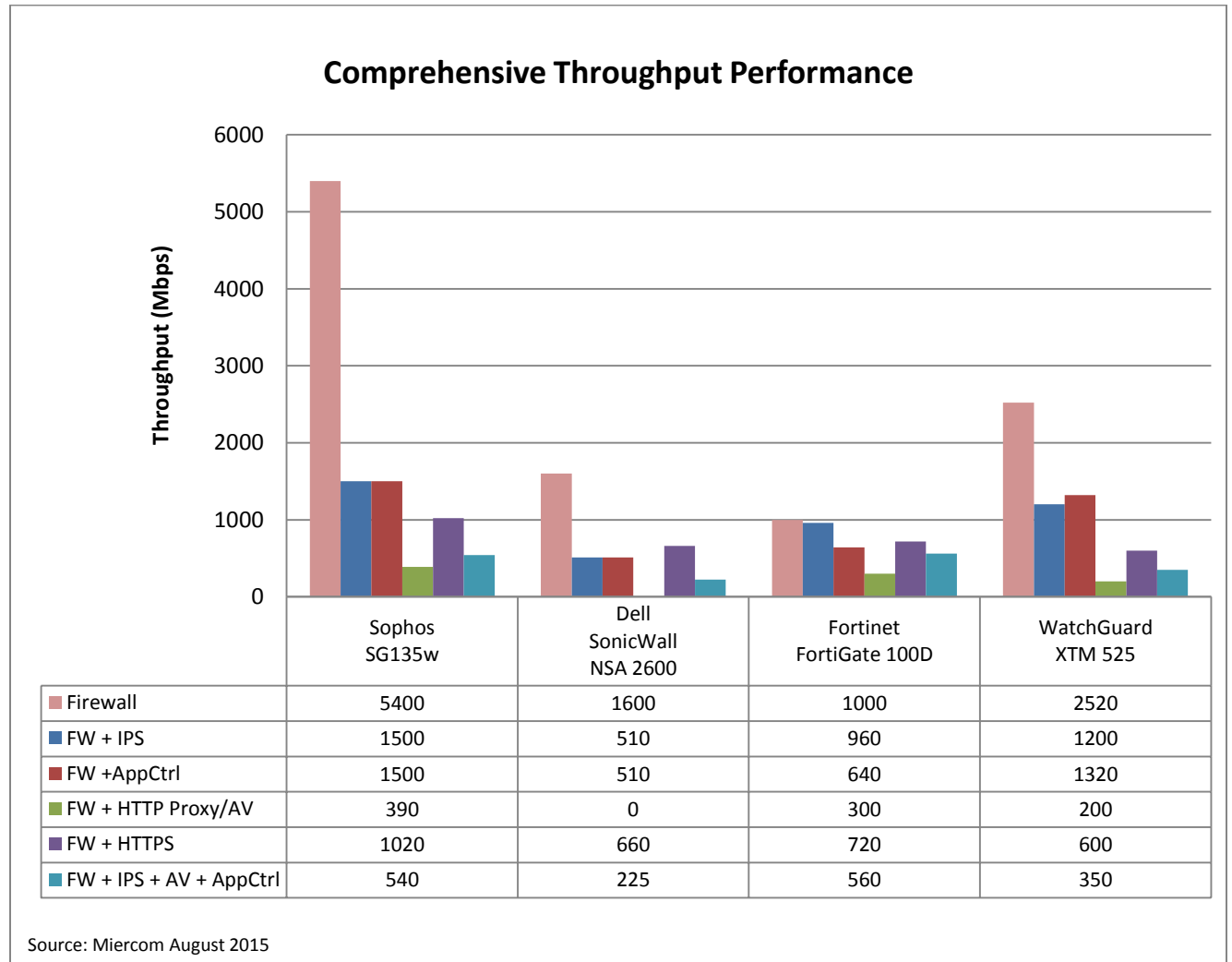
- 1518 byte bidirectional user datagram protocol (UDP): Firewall, IPS, AppCtrl, UTM
- 512 byte bidirectional transmission control protocol (TCP): HTTP Proxy/AV, HTTPS

Throughput Test

Description

The throughput test measured the maximum rate of traffic handled in megabits per second (mps). A test was performed using the firewall only for a baseline measurement. After features were added, tests were conducted to determine what effect they had on performance. The final test represented all features enabled to record UTM mode performance.

Results



The Sophos SG135w had second highest UTM performance with firewall, IPS, AV, and AppCtrl enabled at 540 Mbps, and best performance for the following functions: firewall; firewall and IPS; firewall and HTTP Proxy/AV; and firewall and HTTPS.

Firewall

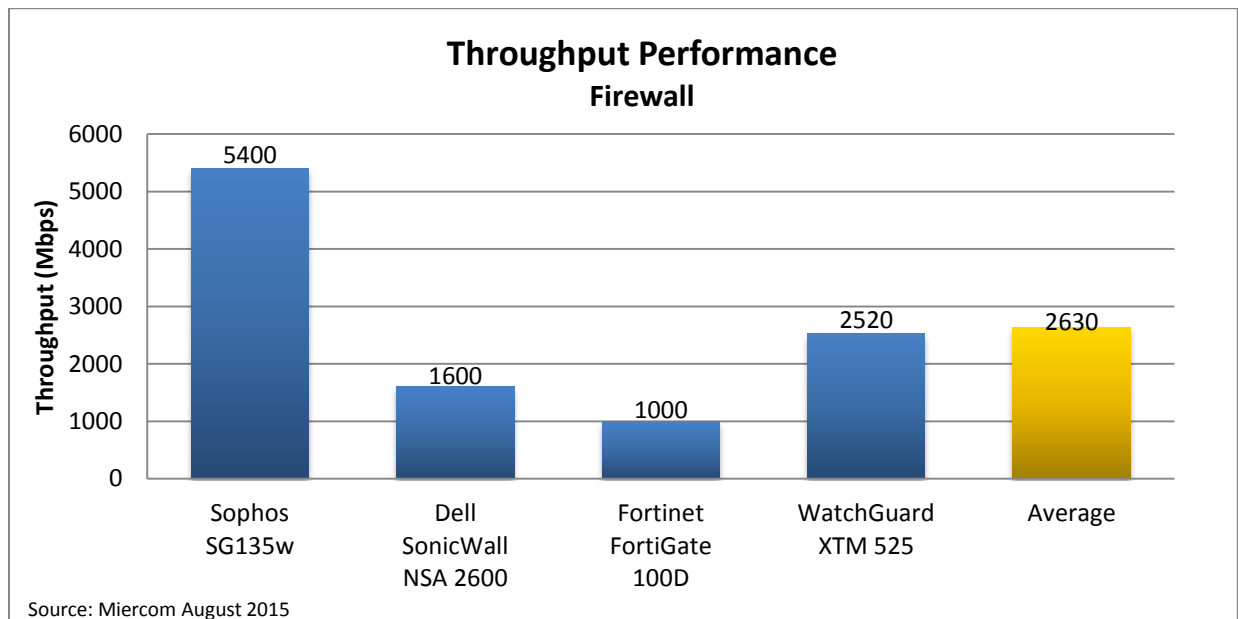
Description

A Firewall is a basic form of protection for a network from external threats. The rates observed in this testing are considered a baseline measurement.

Results

The firewall, the basic mechanism of a UTM device, has higher throughput without security features enabled, since less processing resources are being used.

Firewall Throughput (Mbps)			
Sophos SG135w	Dell SonicWall NSA 2600	Fortinet FortiGate 100D	Watch Guard XTM 525
5,400	1,600	1,000	2,520



The Sophos SG135w had the highest throughput of 5400 Mbps, more than 51% better than the vendor average. Having such a large baseline rate is beneficial since as more features are enabled with the firewall and will predictably reduce throughput, Sophos should continue to maintain a higher rate than the average.

Firewall and Intrusion Prevention System

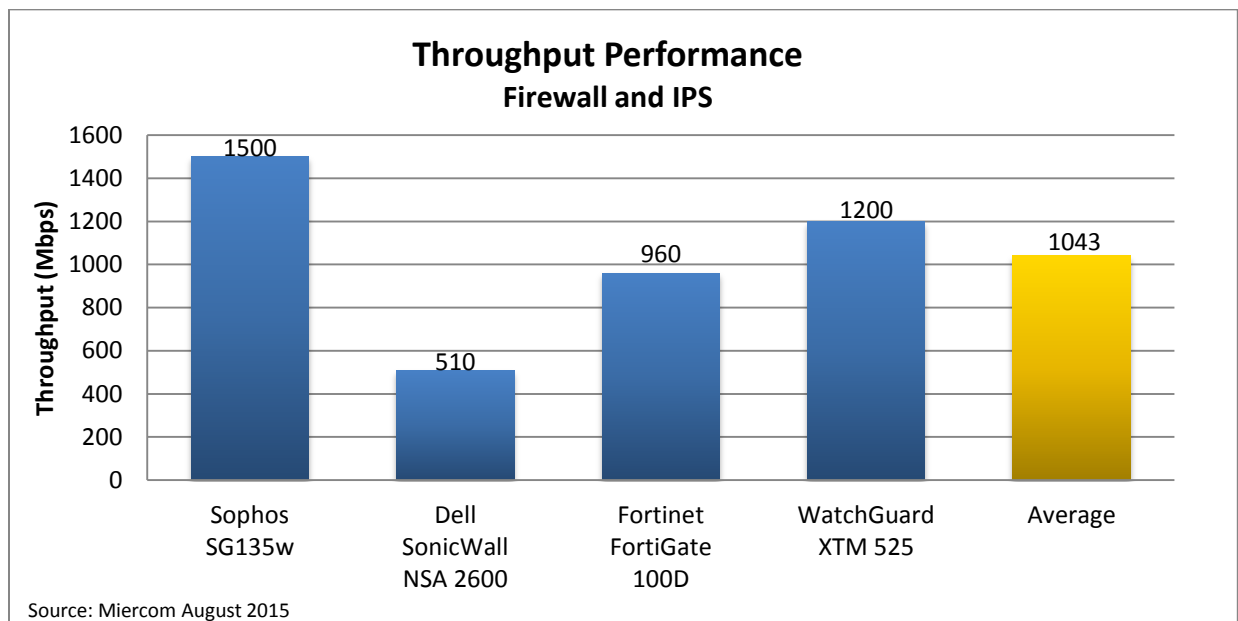
Description

IPS monitors, detects, and blocks threats. Placed in-line, the IPS works to analyze protocol activity using either signature-based, statistical anomaly-based or stateful protocol analysis-based methods for isolating threats from the network. The method chosen for inspection has an effect on processing time and throughput speed.

Results

An IPS method is a refining process that requires additional CPU usage and can affect network performance. It is expected to cause a decrease in throughput.

Firewall and IPS Throughput (Mbps)			
Sophos SG135w	Dell SonicWall NSA 2600	Fortinet FortiGate 100D	Watch Guard XTM 525
1,500	510	960	1,200



The Sophos SG135w saw the highest throughput at 1500 Mbps. Despite a decrease of 72.2% from its baseline firewall throughput, it is still over 30% faster than the vendor average.

Firewall and Application Control

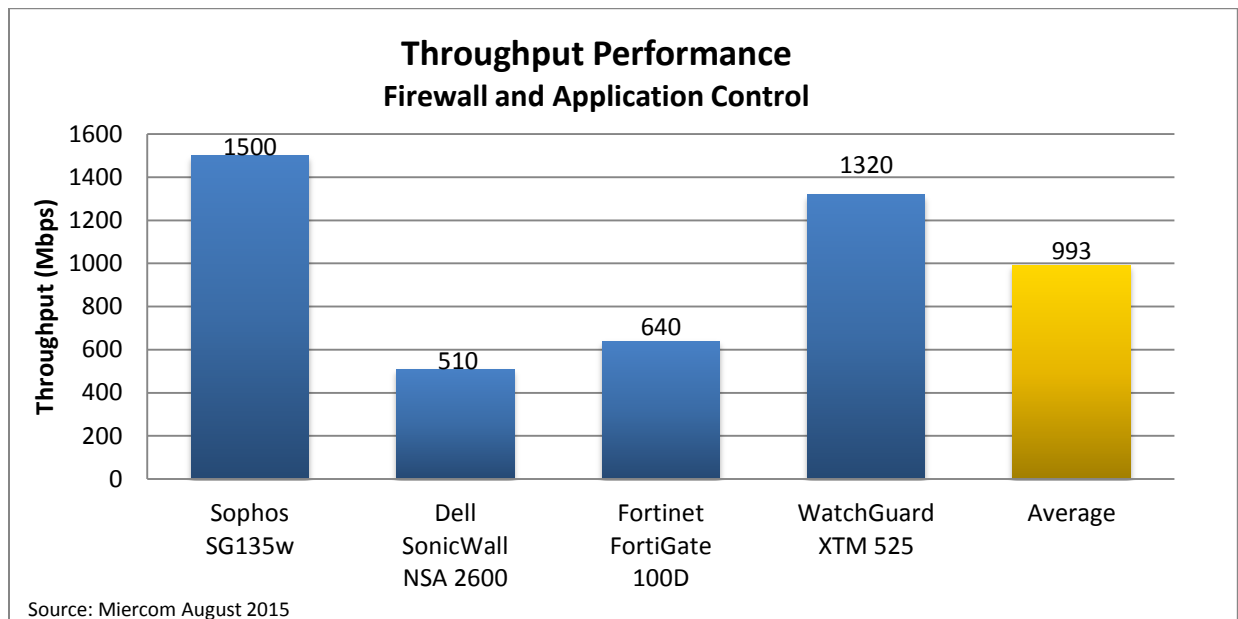
Description

Application control provides regulations and policies to reduce malicious activity. Businesses need to achieve this security measure without degrading network speed. The filtering process places a load on traffic throughput which will cause a decrease.

Results

Application control is expected to slow the throughput rate.

Firewall and Application Control Throughput (Mbps)			
Sophos SG135w	Dell SonicWall NSA 2600	Fortinet FortiGate 100D	Watch Guard XTM 525
1,500	510	640	1,320



The Sophos SG135w had 1500 Mbps, 32% more than the vendor average rate.

Firewall and HTTP Proxy/Antivirus

Description

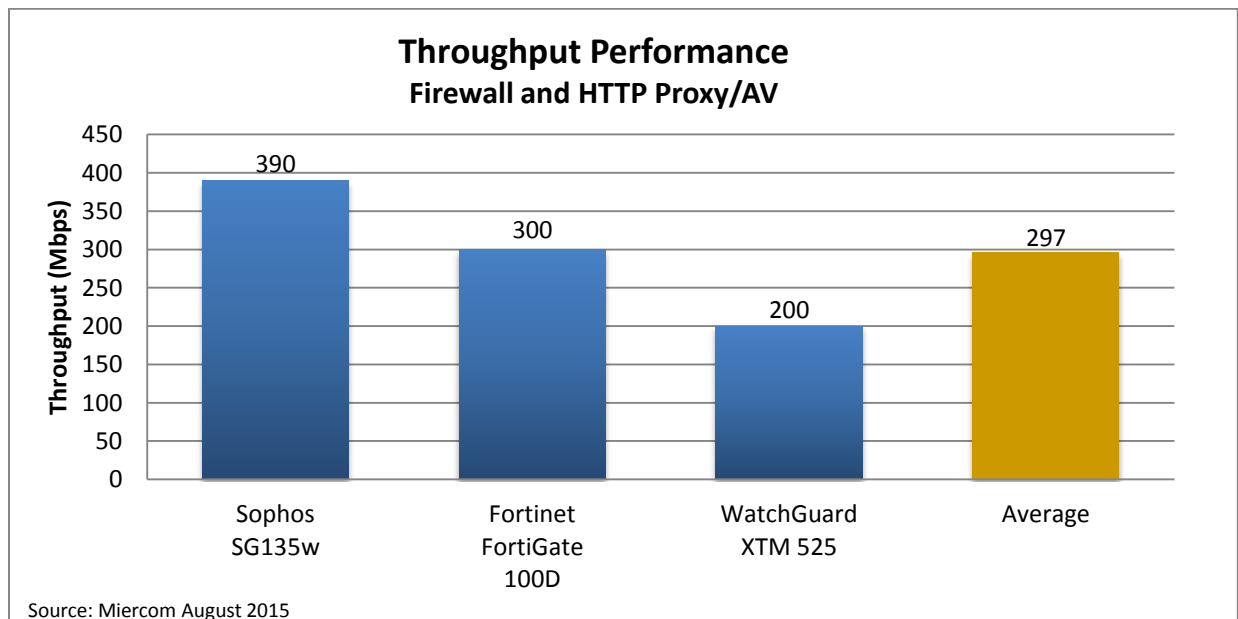
Description

HTTP Proxy/AV adds an extra defense layer against malware attacks via file downloads from websites or file sharing. The proxy buffers the file in memory and scans it from beginning to end with an antivirus engine. This scanning process is done between the handshake of proxy to server, as opposed to a stream-based antivirus scan which examines packets passing through between client and server.

Results

The protocol-based defense will scan and block threats, but this defense layer will significantly reduce throughput.

Firewall and HTTP Proxy/AV Throughput (Mbps)			
Sophos SG135w	Dell SonicWall NSA 2600	Fortinet FortiGate 100D	Watch Guard XTM 525
390	Not Supported	300	200



The Sophos SG135w saw an expected decrease from its baseline, but it continued to have a higher throughput than each competitor. The Sophos SG135w had the highest throughput of 390 Mbps which was 24% more than the vendor average rate.

Firewall and HTTPS

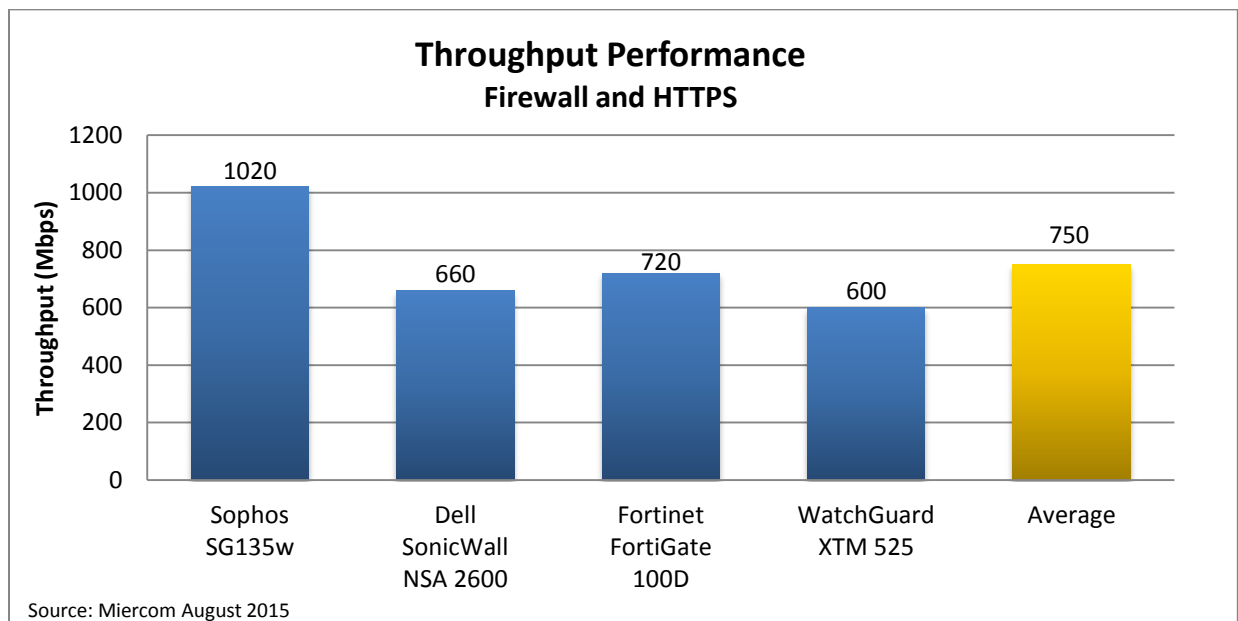
Description

HTTPS is a secured protocol for communications that eliminates vulnerabilities during data transfer. Businesses require all communications to be authentic, untampered and secure, and HTTPS provides a procedure for classifying traffic. However, this protocol requires processing which reduces network speed.

Results

HTTPS requires bidirectional encryption that slows down the processing speed of a network. Throughput is expected to be significantly reduced for this feature.

Firewall and HTTPS Throughput (Mbps)			
Sophos SG135w	Dell SonicWall NSA 2600	Fortinet FortiGate 100D	Watch Guard XTM 525
1020	660	720	600



The Sophos SG135w had the highest throughput of 1020 Mbps, over 26% above the vendor average. Its high rate for secured traffic is significant considering the associated process of encryption is a load that affects network performance.

Unified Threat Management

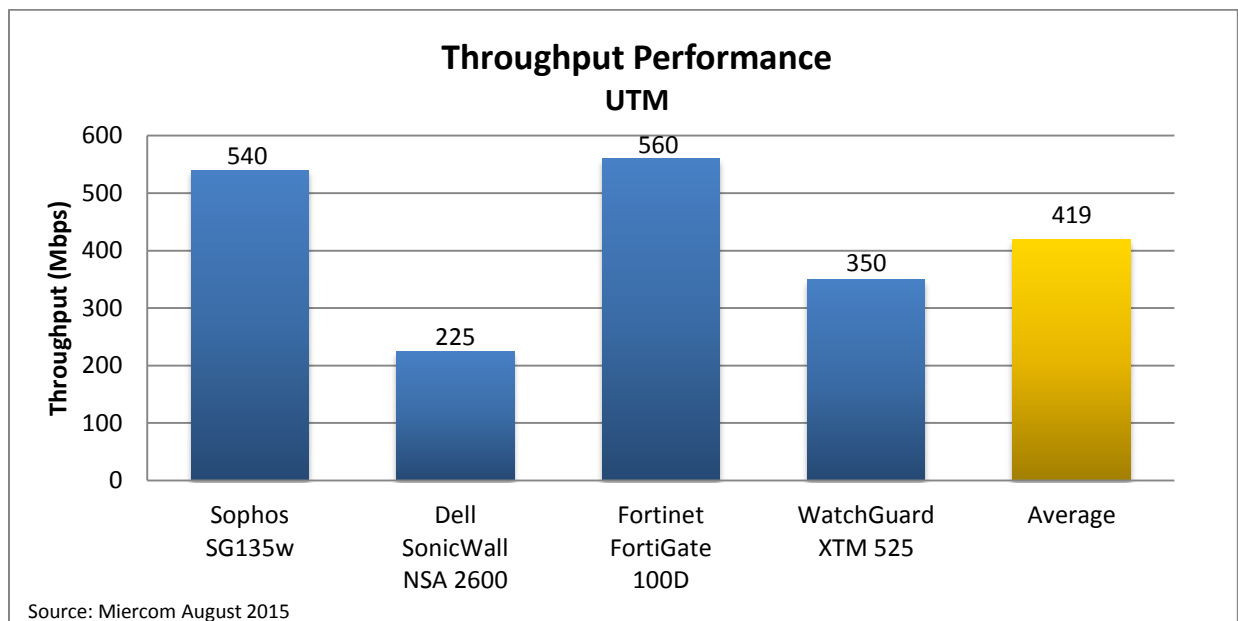
Description

In the UTM mode, all of these features were enabled and running: Firewall, IPS, Application Control, and Antivirus. With all functionality enabled, the increased processing required will cause a significant decrease in throughput performance.

Results

A UTM combines security features' functionalities, which each place a load on network performance, and can be expected to have the lowest throughput performance. Testing was conducted with UDP traffic only to maximize throughput performance rate.

UTM Throughput (Mbps)			
Sophos SG135w	Dell SonicWall NSA 2600	Fortinet FortiGate 100D	Watch Guard XTM 525
540	225	560	350



The Sophos SG135w had the second highest throughput at 540 Mbps, over 22% the vendor average. The Fortinet FortiGate 100D had the highest throughput at 560 Mbps.

Conclusion

The throughput performance of UTM products either as standalone devices or with additional features enabled was measured and discussed in this report. Sophos validated its performance when compared to other vendors in this security industry; particularly how its desktop device performance compared to that of rackmount devices.

The scope of testing included a series of six throughput tests of the following features: firewall, firewall with IPS, firewall with application control, firewall with HTTP proxy/antivirus, firewall with HTTPS, and UTM. These tests were performed on one desktop device from Sophos and three rackmount devices from three vendors: Dell, Fortinet, and WatchGuard. In some instances, the tests could not be performed due to known lack of support for that feature set. These are noted on the appropriate test section with an explanation.

It is clear to see that deploying additional features does affect the throughput in all cases, as is expected. It is interesting to see which additional security features causes the most impact. Security comes at a price, not just in dollars, but in the ability of the network to handle traffic while maintaining security.

Overall, the performance of the Sophos SG135w desktop device was better than most rackmount products. Additionally, Sophos has a quick and simple set up. Configuration was very straightforward, and the graphical user interface (GUI) was clean and easy to navigate with a minor learning curve. A unique feature was interface cloning, making last minute changes and customization much more simple and intuitive to deploy.

The Sophos SG135w meets the security needs of a network, while maintaining the performance required in a networking environment.

Fair Test Notification

All vendors with products featured in this report were afforded the opportunity before, during, and after testing was complete to comment on the results and demonstrate the performance of their product(s). Any vendor with a product tested by Miercom in one of our published studies that disagrees with our findings is extended an opportunity to retest and demonstrate the performance of the product(s) at no charge to the vendor. All vendors are welcome to demonstrate their product performance on their own to Miercom. These results will be updated if new data presents itself.

In this evaluation Miercom testing used HTTP, 1518 byte bidirectional UDP traffic, while WatchGuard in their own test bed used multiple HTTP GET requests for a 1 MB file, which allowed them to demonstrate better performance. However, Miercom used the same configuration for all vendors tested.

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.

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.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Miercom or Sophos. 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.