Unified Threat Management Throughput Performance

Desktop Device Comparison

DR160101D

May 2016

Miercom
www.miercom.com

Contents

Copyright © 2016 Miercom

Executive Summary

Miercom was engaged by Sophos to conduct independent performance testing of the Sophos *XG 135W* unified threat management (UTM) desktop firewall as a network security solution. Testing, which employed industry-leading performance testing equipment, was conducted competitively against Check Point 2200, Dell SonicWall TZ600, Fortinet FortiGate 90D and WatchGuard M200 in February 2016.

This report explains the load impact on network performance by using the following scenarios:

- **Baseline performance.** Firewall throughput was tested using various packet sizes on the UTM. The most efficient packet size, 1518 was used for all subsequent testing.
- **Firewall with other security features enabled.** Additional functions were individually applied to evaluate how these impacted the performance of the UTM.
- **Full UTM mode**. Firewall baseline with all functions enabled (intrusion prevention, application control and antivirus) showing true UTM performance.

Each device was also tested to determine maximum connection and concurrent connection rates. Connection dynamics provide an important role in properly sizing a security device.

Throughput results for all tests were recorded and compared with competitive products and their averages. All results shown in this report are based on actual observations in our lab.

Key Findings

- Baseline firewall throughput was 6,560 Mbps, outperforming the average by 67%
- Throughput was highest for firewall, firewall with application control enabled, firewall with HTTP Proxy/Antivirus enabled and full UTM mode against all vendors.
- UTM throughput at 560 Mbps is 31% above the competitive average
- Connection rate and concurrent connection rates were 66.1% and 92% higher than the competitive average, respectively

Overall The Sophos XG 135W had better performance metrics when compared to the vendor's averages in UTM mode.

Based on the results of our testing, the Sophos XG 135W UTM desktop solution is capable of high throughput, fast connection rate and ability to handle numerous concurrent endpoints, earning the Miercom Performance Verified certification.

Robert Smithers
CEO
Miercom

Copyright © 2016 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	*Controls and filters flow of traffic within a network with a barrier to protect trusted internal network from an unsecure network (e.g. Internet)*
Intrusion Prevention System	IPS	*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.*
Application Control	AppCtrl	*Enforces policies regarding security and resources by restricting/controling which applications can traverse through the UTM. It intends to reduce occurrences of infection, attacks, and negative consequences of malicious content.*
Hypertext Transfer Protocol Proxy/Antivirus	HTTP Proxy/AV	*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.*
Hypertext Transfer Protocol Secure	HTTPS	*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.*
Unified Threat Management	UTM	*All-inclusive security with multiple functions in central unit. Contains firewalling, IPS, AV, VPN, content filtering, and sensitive data loss prevention.*

Copyright © 2016 Miercom

UTM devices contain the same functionality as Next-Generation Firewall and Secure Web Gateway devices, 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 desktop models and compared.

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

Competitor Average

The competing UTM devices are averaged for comparison to the Sophos XG 135W. These averages serve as a reference for the performance results recorded for the Sophos product.

Copyright © 2016 Miercom

Products Tested

Product Name	Version
Sophos XG 135W	15.01.0
CheckPoint 2200	R77.20
Dell SonicWall TZ600	6.2.3.0-ISN
Fortinet FortiGate 90D	5.4.0
WatchGuard M200	11.10.5.B492938

Sophos

The *Sophos XG 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. All XG Firewalls support high availability and can be centrally managed through Sophos Firewall Manager. This UTM allows protection to be added as needed, through software upgrades, without additional hardware.

Check Point

The *Check Point 2200* is a consolidated solution for small businesses and branch offices that provides networks with attack detection and prevention. Its layered defense uses ThreatCloud sandboxing, generates signatures for current malicious behavior, and blocks suspicious activity from entering a network. The ThreatCloud shares these signatures with all Check Point customers, creating global protection.

Dell

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

Fortinet

The *Fortinet FortiGate 90D* protects distributed network locations with its core management system consisting of its proprietary software for firewall, IPS, VPN, and filtering control over network traffic.

WatchGuard

The *WatchGuard M200* is geared towards small businesses looking for flexible management of network activity. Features supported are firewall, VPN, IPS and reputation-based antivirus. Routing is policy based, and reporting is simple. Power consumption is built with environmentally friendly efficiency.

Copyright © 2016 Miercom

How We Did It

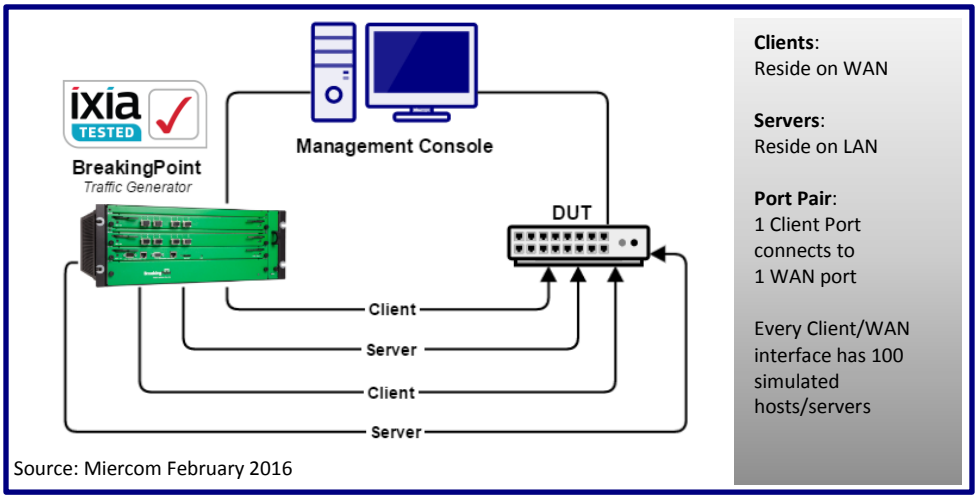
The impact of security on network performance is a key component of this test methodology. Miercom simulated a robust and realistic testing environment to determine performance of each device under different use cases. Devices were configured for optimal functionality to enable maximum throughput, while the security features were deployed.

The following test cases were simulated:

- Firewall Throughput with Different Frame Size
  - 1518 byte traffic (baseline)
  - 512 byte traffic
  - 64 byte traffic
  - IMIX traffic
- Firewall + IPS
- Firewall + Application Control
- Firewall + HTTP Proxy/AV
- Firewall + HTTPS
- UTM
- Max Connections per second
- Max Concurrent Connections per second

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

Test Bed Setup



Traffic was sent to each security device through a WAN port and received through a LAN port. The number of WAN and LAN ports used depended on the maximum available on each device.

BreakingPoint clients were external and connected to the WAN port of the DUT. *BreakingPoint* servers were our protected clients and connected to the LAN port of the DUT.

Copyright © 2016 Miercom

Traffic Generation

The *Ixia BreakingPoint Firestorm 20* generated traffic for each device under test. The traffic represented a real-world, high-stress 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:

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

Throughput performance of each device under varying loads was recorded until a maximum was achieved. Maximum was noted when the device began dropping packets, signaling a fail in traffic delivery.

Ixia BreakingPoint FireStorm20

Other 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

It 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

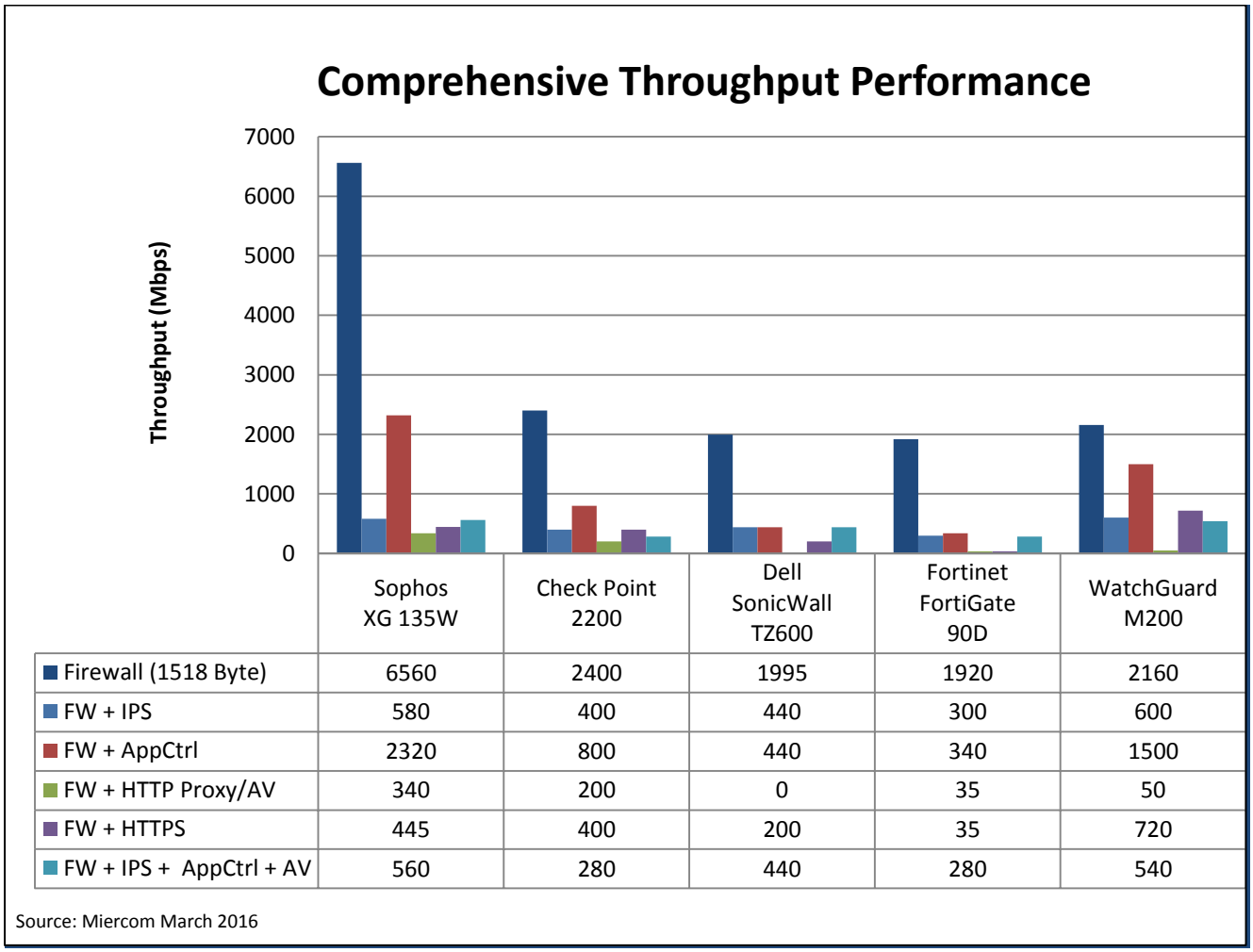
Copyright © 2016 Miercom

Throughput Tests

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



	Sophos XG 135W	Check Point 2200	Dell SonicWall TZ600	Fortinet FortiGate 90D	WatchGuard M200
Firewall (1518 Byte)	6560	2400	1995	1920	2160
FW + IPS	580	400	440	300	600
FW + AppCtrl	2320	800	440	340	1500
FW + HTTP Proxy/AV	340	200	0	35	50
FW + HTTPS	445	400	200	35	720
FW + IPS + AppCtrl + AV	560	280	440	280	540

Source: Miercom March 2016

The Sophos XG 135W had the best UTM performance with IPS, AppCtrl and AV enabled at 560 Mbps, and best performance for the following functions: firewall; firewall and application control; and firewall and HTTP Proxy/AV.

Copyright © 2016 Miercom

Firewall

A firewall is a basic form of protection for a network from external threats. Its performance was evaluated for traffic containing different Ethernet IEEE 802.3 standard packet frame sizes.

1518 byte	This is the largest frame size to hold the most packets of data. With more bandwidth, the DUT has to work less to retrieve data and scan for malicious activity. This frame size is expected to yield the highest throughput rate. This is the baseline for the UTM test.
512 byte	As a moderate frame size it holds less data, but it maintains sufficient bandwidth. The DUT works harder to sift through more frames to scan for abnormalities and is expected to have a lower throughput rate than with 1518 byte traffic.
64 byte	This is the smallest frame size, and by having smaller bandwidth it must take more frames to transmit packets of data. This segmentation forces the DUT to work the hardest to scan and is expected to have the lowest bandwidth.
IMIX	A mixture of frame sizes contains percentages of each of the preceding frame sizes. The IMIX traffic used in testing had unknown percentages and random sequence of order. It was expected to have very low throughput but at a higher rate than the pure 64 byte traffic.

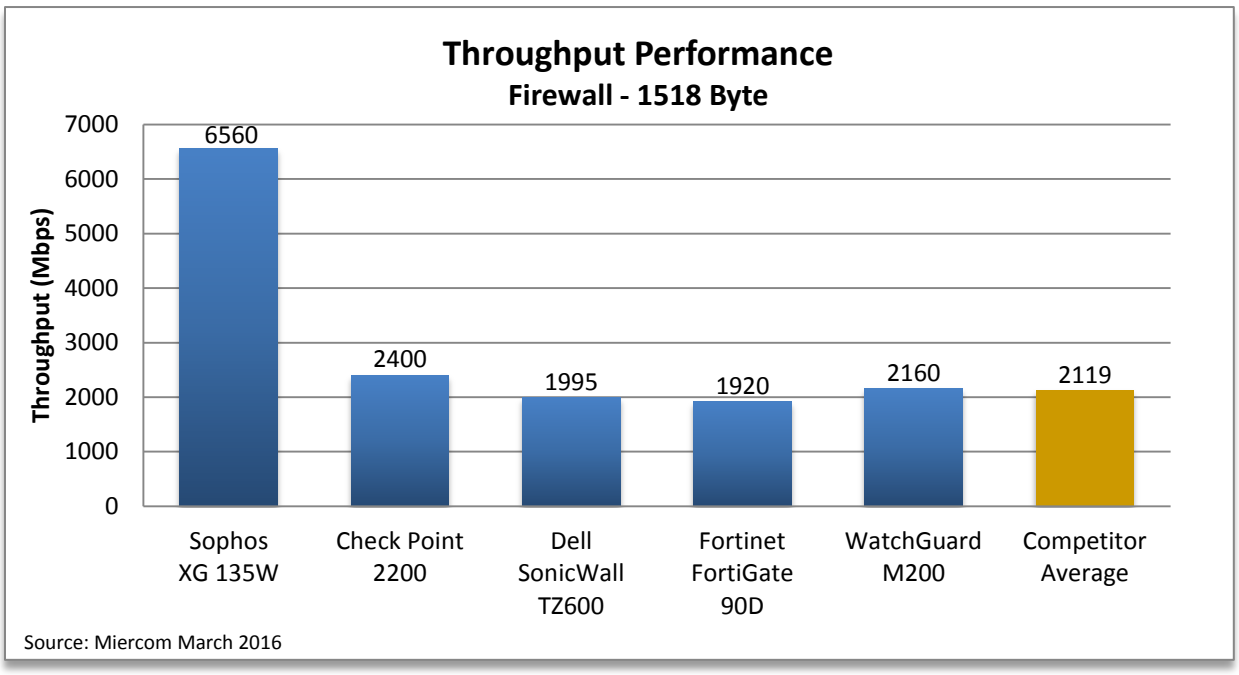
The 1518-byte packet size was used as the baseline for subsequent tests where different features were applied since it would imply the best-case scenario for the DUT. The firewall, the basic mechanism of a UTM device, has higher throughput without security features enabled, since less processing resources are being used.

Copyright © 2016 Miercom

Results

This throughput serves as the baseline for each device. When features are added to its functionality, this throughput is expected to decrease.

1518 Byte Packet Frame Firewall Throughput (Mbps)				
Sophos XG 135W	Check Point 2200	Dell SonicWall TZ600	Fortinet FortiGate 90D	Watch Guard M200
6,560	2,400	1,995	1,920	2,160

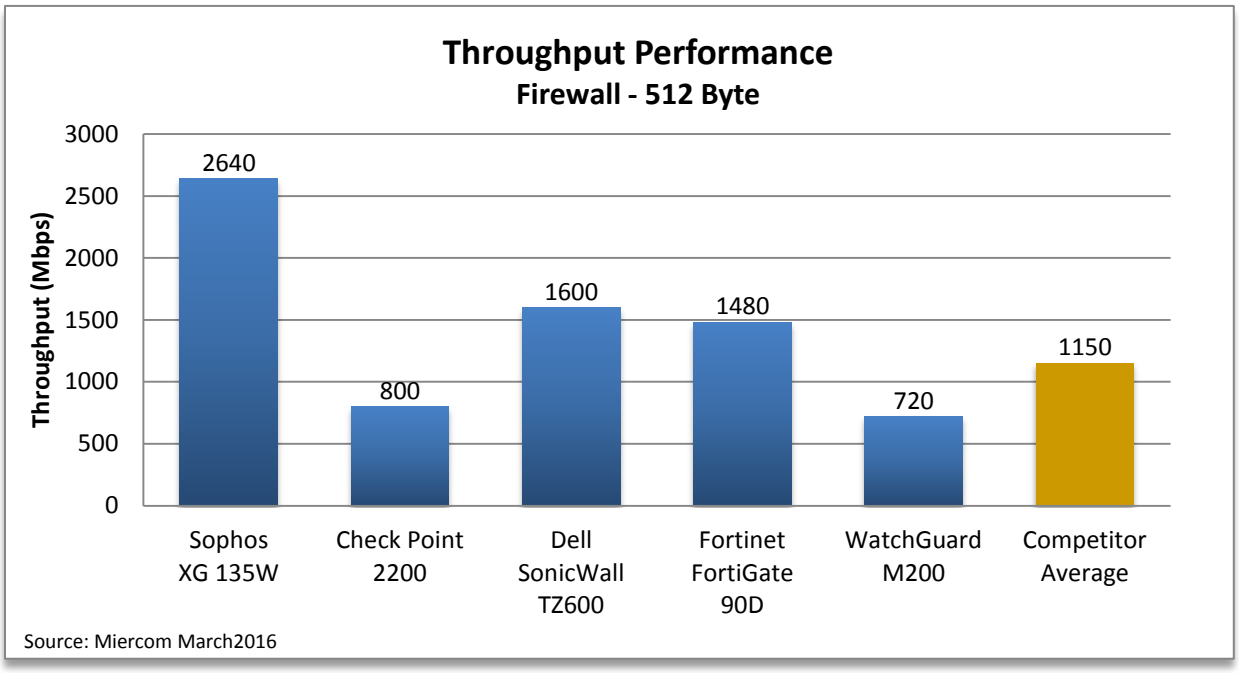


The Sophos XG 135W set its baseline throughput with firewall enabled at 6560Mbps, 67.7% more than the competing vendor average. Having such a large baseline rate is beneficial since as more features are enabled with the firewall and will predictably reduce throughput, Sophos should continue to maintain a higher rate than the average.

Copyright © 2016 Miercom

This throughput is significantly lower than that of the 1518 byte traffic.

512 Byte Packet Frame Firewall Throughput (Mbps)				
Sophos XG 135W	Check Point 2200	Dell SonicWall TZ600	Fortinet FortiGate 90D	WatchGuard M200
2,640	800	1,600	1,480	720

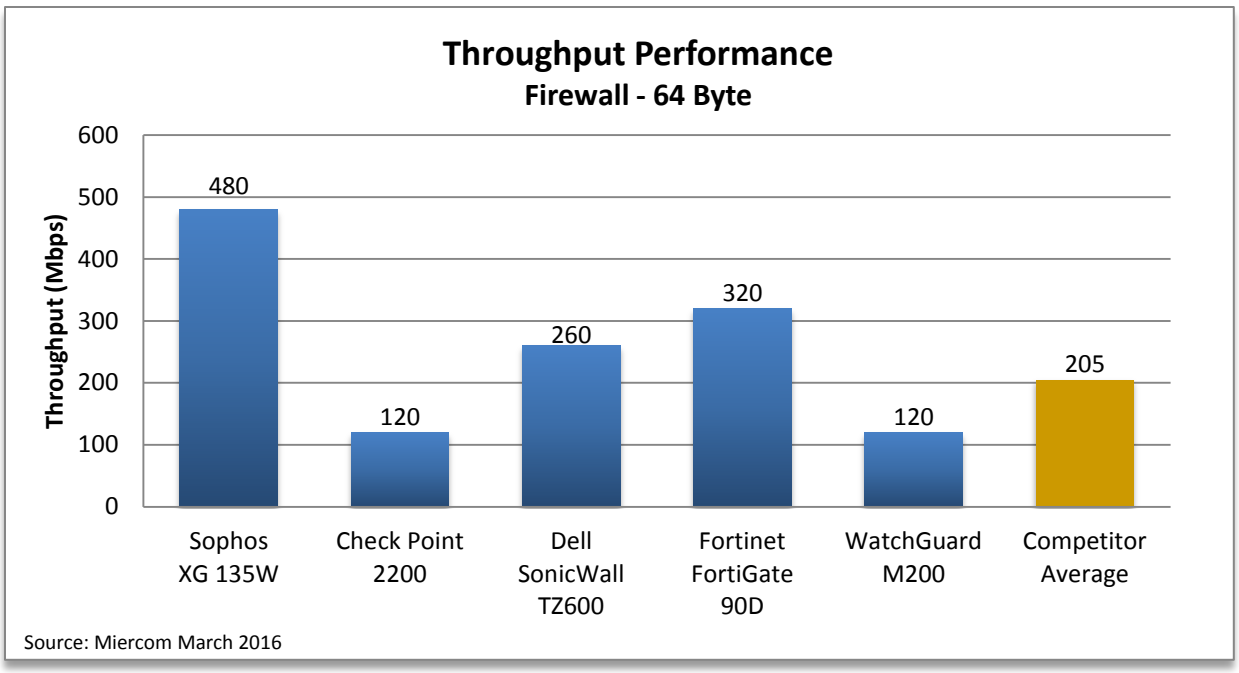


The Sophos XG 135W saw a decrease in throughput when traffic frame size was reduced. With smaller bandwidth, the device has more frames of packets to scan. As expected, it remained 56% higher than the vendor average and the highest of all individual vendors.

Copyright © 2016 Miercom

This traffic has the smallest frame size and requires the most effort from each device. As expected, it has the lowest throughput.

64 Byte Packet Frame Firewall Throughput (Mbps)				
Sophos XG 135W	Check Point 2200	Dell SonicWall TZ600	Fortinet FortiGate 90D	WatchGuard M200
480	120	260	320	120

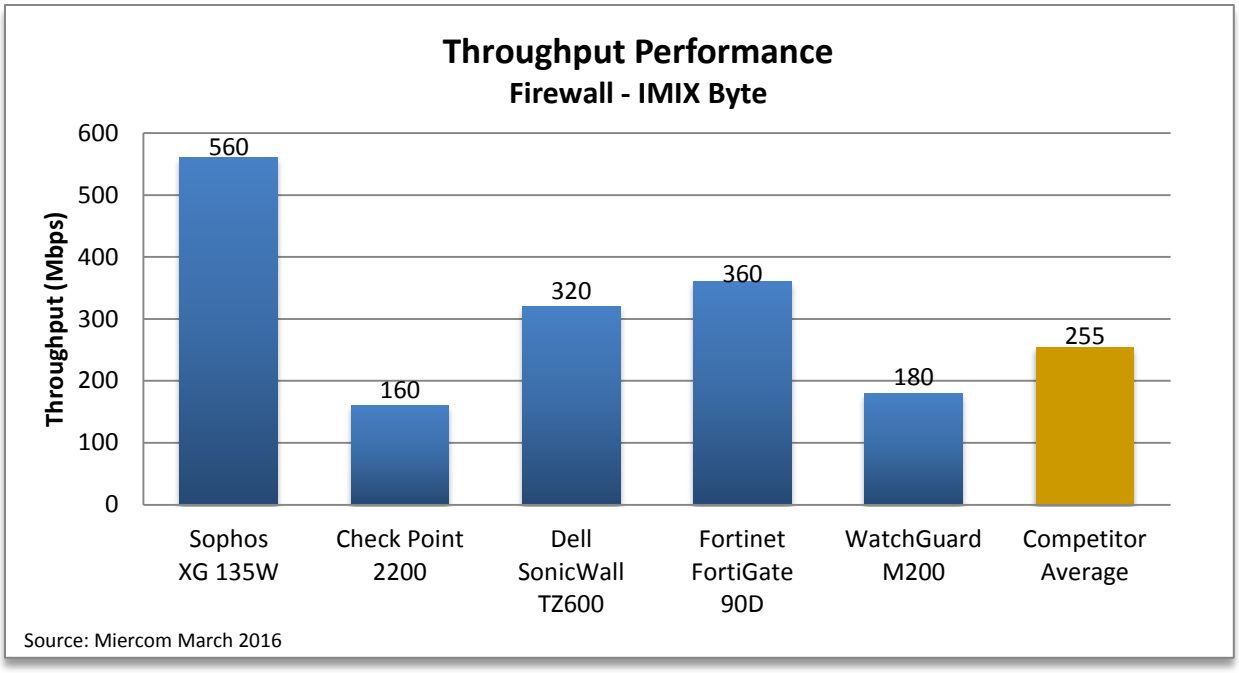


The Sophos XG 135W had the highest throughput of all vendors and saw an expected decrease in throughput when packet size was reduced to 64 byte. With such limited bandwidth, the device works harder to scan the same amount of data in previous tests of 1518 byte and 512 byte frame sizes. The throughput was still 57% higher than the competitive average.

Copyright © 2016 Miercom

The mixture of traffic yields results that are better than the lowest frame size throughput rate but not as high as the 512 byte or 1518 byte traffic.

IMIX Packet Frame Firewall Throughput (Mbps)				
Sophos XG 135W	Check Point 2200	Dell SonicWall TZ600	Fortinet FortiGate 90D	WatchGuard M200
560	160	320	360	180



The Sophos XG 135W displays better throughput for IMIX traffic than the smallest frame size of 64 bytes since it is a mixture of all frame sizes with no reference to the amount of each type or the order. In comparison to the vendor average, it had more than 55% of a higher rate and was the highest of every individual vendor.

Copyright © 2016 Miercom

Firewall and Intrusion Prevention System

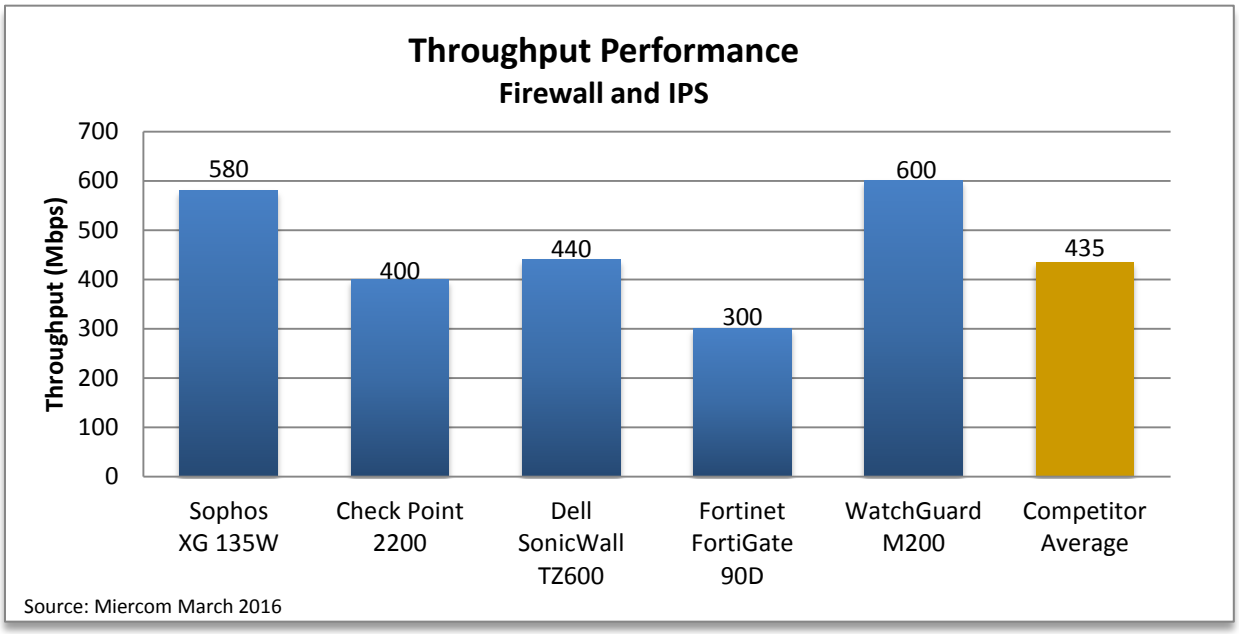
IPS monitors, detects, and blocks threats. Placed in-line, the IPS works to analyze protocol activity using either signature-based, statistical anomaly-based or stateful protocol analysis-based methods for isolating threats from the network. The method chosen for inspection has an effect on processing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

This test evaluates the DUT for its throughput rate when firewall and IPS features are enabled under 1518 byte traffic.

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 the baseline throughput.

Firewall and IPS Throughput (Mbps)				
Sophos XG 135W	Check Point 2200	Dell SonicWall TZ600	Fortinet FortiGate 90D	WatchGuard M200
580	400	440	300	600



The throughput rate of the Sophos XG 135W was 25% higher than the vendor average. As expected, all vendors' throughput rates declined from their baseline. The vendor average fell by 86%.

Copyright © 2016 Miercom

Firewall and Application Control

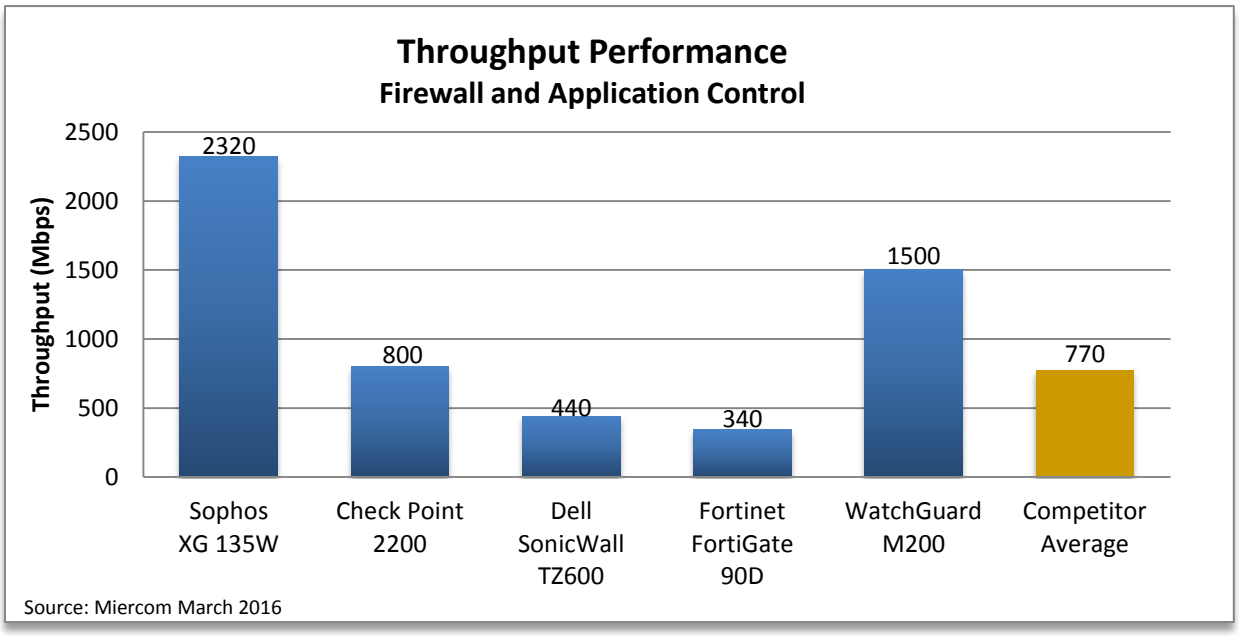
Application control provides regulations and policies to reduce malicious activity. Businesses need to achieve this security measure without degrading network speed. The filtering process places a load on traffic throughput which will cause a decrease.

This test evaluates the DUT for its throughput rate when firewall and application control features are enabled under 1518 byte traffic.

Results

Application control is expected to slow the throughput rate.

Firewall and Application Control Throughput (Mbps)				
Sophos XG 135W	Check Point 2200	Dell SonicWall TZ600	Fortinet FortiGate 90D	WatchGuard M200
2,320	800	440	340	1,500



The Sophos XG 135W had the highest throughput, 67% higher than the competing vendor average.

Copyright © 2016 Miercom

Firewall and HTTP Proxy/Antivirus

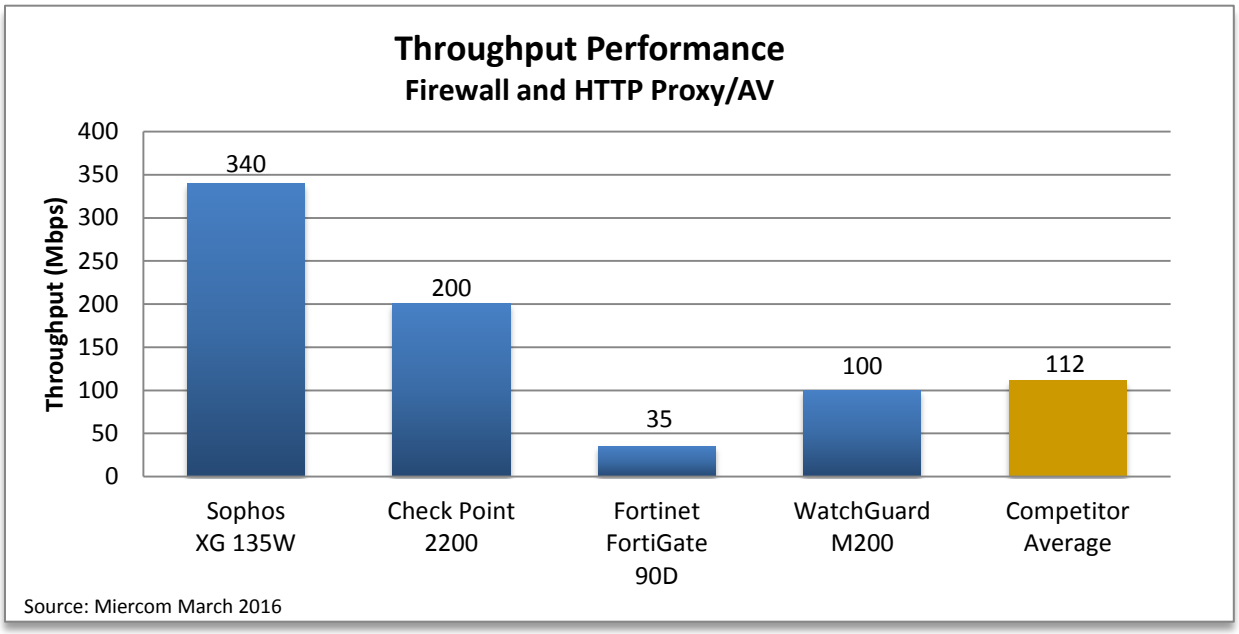
HTTP Proxy/AV adds an extra defense layer against malware attacks via file downloads from websites or file sharing. The proxy buffers the file in memory and scans it from beginning to end with an antivirus engine. This scanning process is done between the handshake of proxy to server, as opposed to a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

This test evaluates the DUT for its throughput rate when firewall and HTTP Proxy/Antivirus features are enabled under 1518 byte traffic.

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 XG 135W	Check Point 2200	Dell SonicWall TZ600	Fortinet FortiGate 90D	WatchGuard M200
340	200	Not Supported	35	100



The Sophos XG 135W had the highest performance against its competitors, more than 67% higher than the average. The HTTP Proxy/AV feature is the most intensive load as shown by each vendor's decrease from their baseline.

Copyright © 2016 Miercom

Firewall and HTTPS

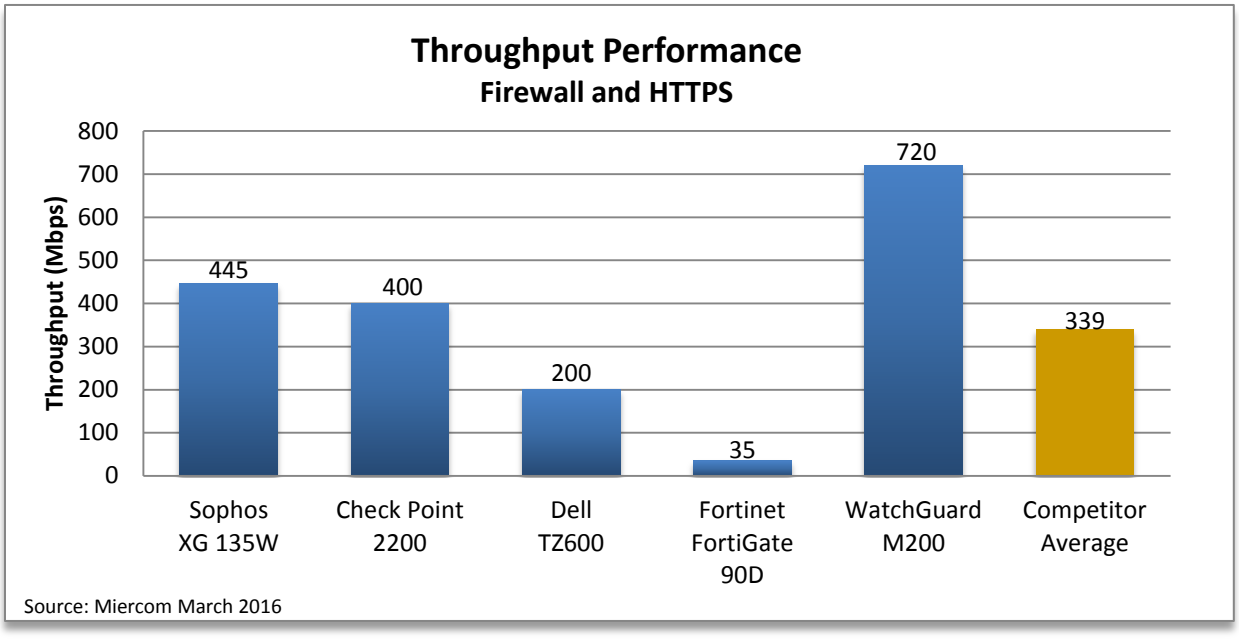
HTTPS is a secured protocol for communications that eliminates vulnerabilities during data transfer. Businesses require all communications to be authentic, untampered and secure, and HTTPS provides a procedure for classifying traffic. However, this protocol requires processing which reduces network speed.

This test evaluates the DUT for its throughput rate when firewall and HTTPS features are enabled under 1518 byte traffic. Competitive products were tested using stream-based inspection, while the Sophos XG 135W used proxy-based inspection. While proxy based inspection normally yields lower throughput, it allows for more thorough inspection for threats.

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 XG 135W	Check Point 2200	Dell SonicWall TZ600	Fortinet FortiGate 90D	WatchGuard M200
445	400	200	35	720



The Sophos XG 135W saw sufficient impact from the HTTPS feature, but it was still higher than the competing average by 24%. The HTTPS feature requires encryption and decryption capabilities which affect throughput performance.

Copyright © 2016 Miercom

Unified Threat Management

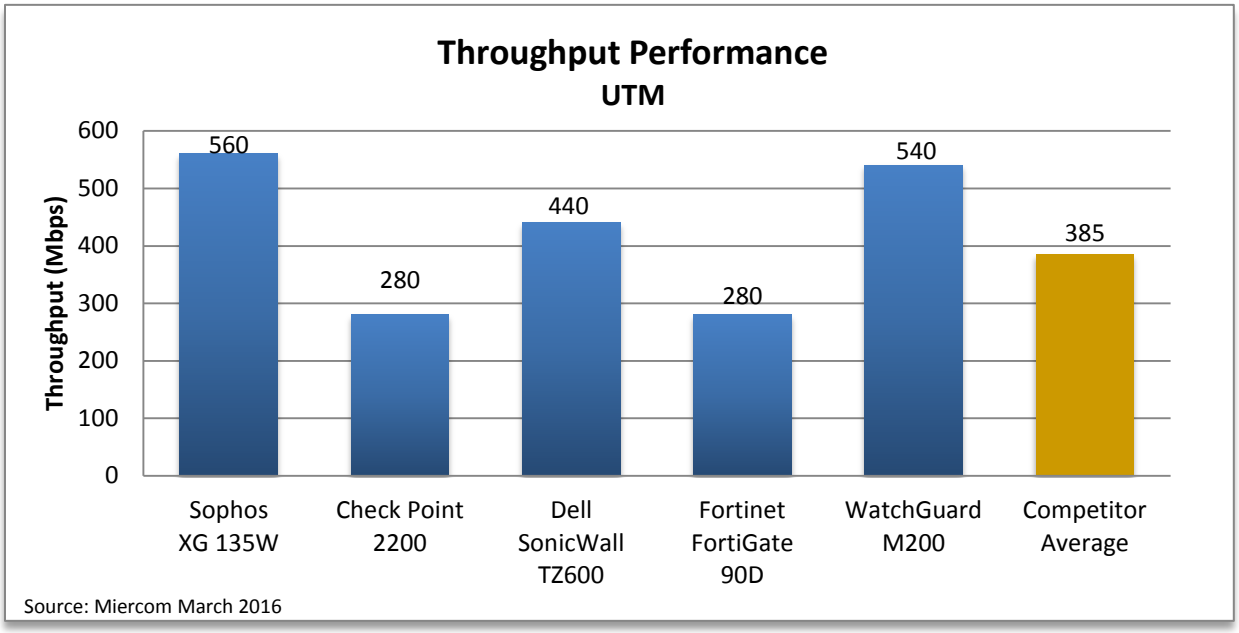
In the UTM mode, all of these features were enabled and running: Firewall, IPS, Application Control, and Antivirus. With all functionality enabled, the increased processing required will cause a significant decrease in throughput performance.

This test evaluates the DUT for its throughput rate when firewall, IPS, application control and HTTP/AV features are enabled under 1518 byte traffic.

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 XG 135W	Check Point 2200	Dell SonicWall TZ600	Fortinet FortiGate 90D	WatchGuard M200
560	280	440	280	540



In full UTM mode, the Sophos XG 135W claims the highest performance rate. Its throughput surpasses the competitive performance by 31.3%.

Copyright © 2016 Miercom

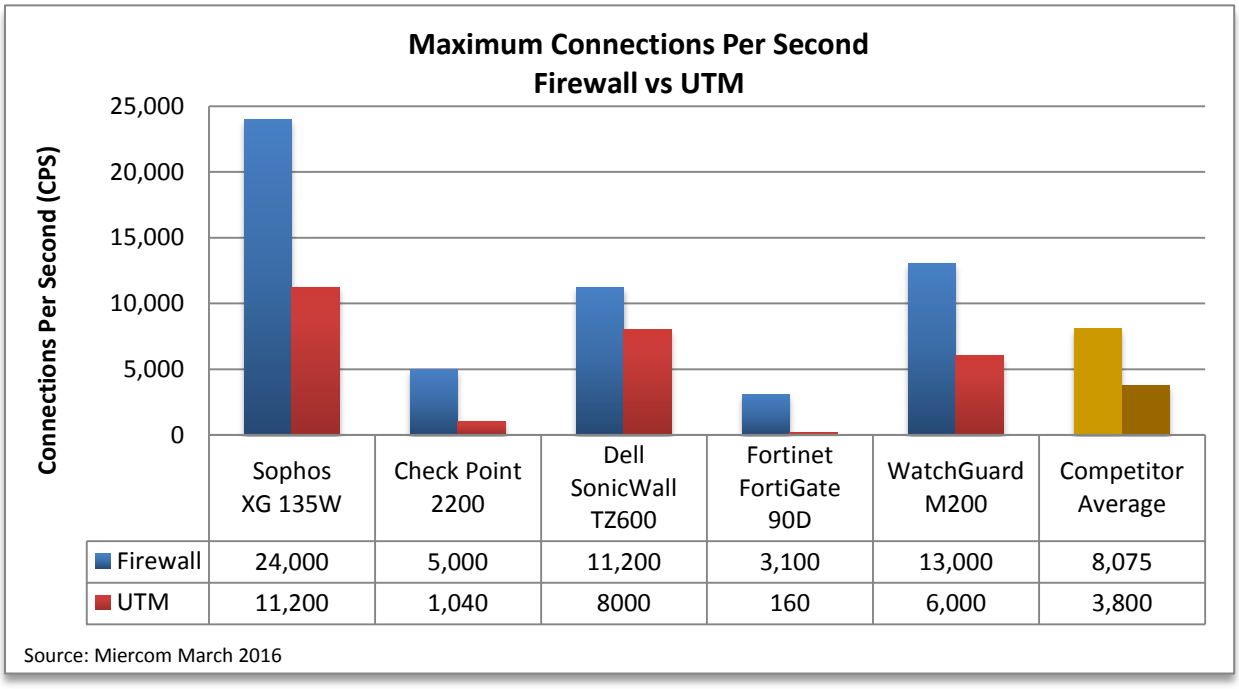
Maximum Connections per Second

Connections per second (CPS) is the rate at which the device can make new connections. This rate is related to processor speed, memory speed and architecture. This rate is compared at the baseline (firewall with 1518 byte frame size traffic) and full UTM (firewall at 1518 bytes, IPS, application control and AV).

Results

Each device is expected to have a lower connection rate when UTM features are enabled.

1518 byte Firewall Max CPS				
Sophos	Check Point	Dell	Fortinet	WatchGuard
24,000	5,000	11,200	3,100	13,000
1518 byte UTM Max CPS				
Sophos	Check Point	Dell	Fortinet	WatchGuard
11,200	1,040	8,000	160	6,000
Performance Impact (CPS)				
Sophos	Check Point	Dell	Fortinet	WatchGuard
-12,800	-3,960	-3,200	-2,940	-7,000



The Sophos XG 135W baseline maximum CPS was 66.4% higher than the competitor average. Its UTM maximum decreased by 12,800 CPS and was 66.1% higher than the average UTM.

Copyright © 2016 Miercom

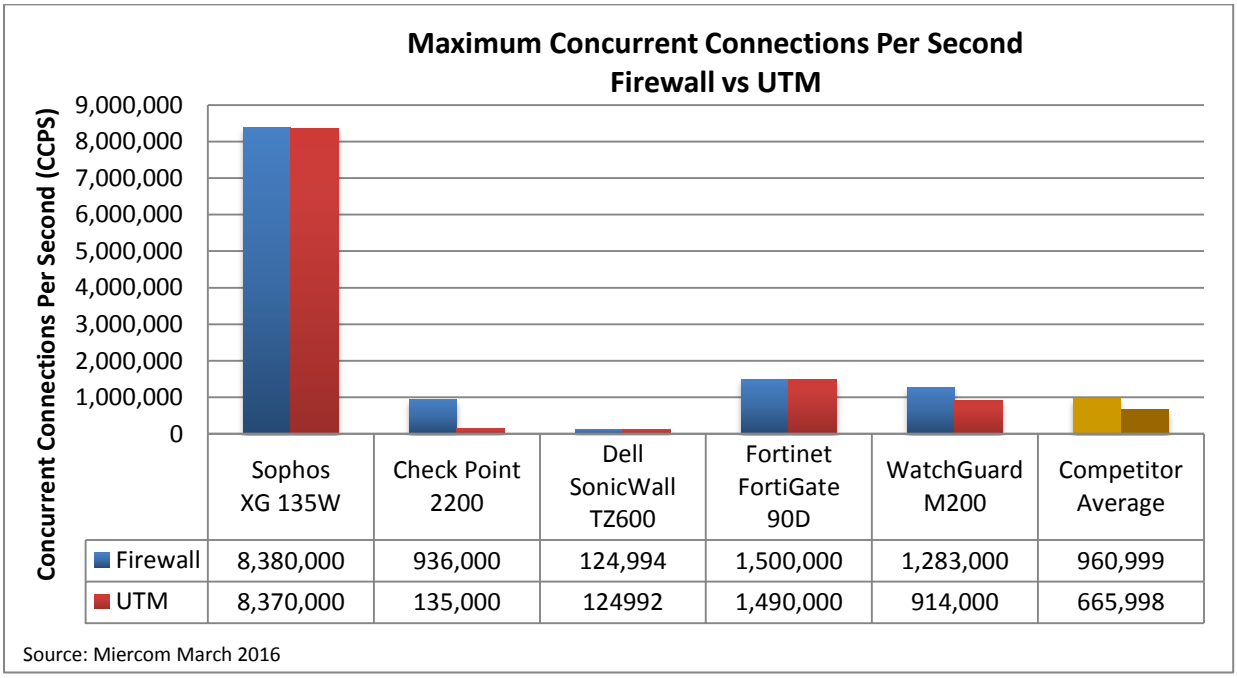
Maximum Concurrent Connections per Second

Concurrent connections per second (CCPS) is the rate at which the device can maintain connections simultaneously and is related to the amount of memory for the DUT. This rate is compared at the baseline (firewall with 1518 byte frame size traffic) and full UTM (firewall at 1518 bytes, IPS, application control and AV).

Results

Each device is expected to have a lower connection rate when UTM features are enabled.

1518 byte Firewall Max CPS				
Sophos	Check Point	Dell	Fortinet	WatchGuard
8,380,000	936,000	124,994	1,500,000	1,283,000
1518 byte UTM Max CPS				
Sophos	Check Point	Dell	Fortinet	WatchGuard
8,370,000	135,000	124,992	1,490,000	914,000
Performance Impact (CPS)				
Sophos	Check Point	Dell	Fortinet	WatchGuard
-10,000	-801,000	-2	-10,000	-369,000



Source: Miercom March 2016

The Sophos XG 135W baseline maximum CCPS was 88.5% higher than the competitor average. Its UTM maximum decreased by 10,000 CCPS and was 92% higher than the average. Its concurrent connection rate was extremely high but also had a fairly insignificant decrease when all UTM features were applied.

Copyright © 2016 Miercom

Conclusion

The Sophos XG 135W UTM desktop appliance and competing UTM vendors were evaluated for their performance under realistic, high-stress network scenarios. The focus of this report was to demonstrate the capability of the Sophos device and how it compares to these similar products.

The scope of testing included a series of six throughput tests and two connection rate tests. Throughput tests consisted of the following: 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 four desktop devices from four vendors: Check Point, 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. Connection rate tests were for the following: maximum connections per second for firewall and UTM and maximum concurrent connections per second for firewall and UTM.

The Sophos XG 135W had the highest throughput rate for different firewall test cases, which differed in the frame size of traffic being sent to the DUT. Its highest throughput was its baseline, performing at 6,650 Mbps.

With additional features enabled, the Sophos device performed better than the competitive average for each test. Its UTM performance was 560 Mbps, over 25% the average throughput. The performance was measured and discussed in this report. Sophos validated its performance when compared to other vendors in this security industry.

Its connection rate, for new connections and concurrent connections, was higher than its competitors and decreased an expected amount from its baseline; this had little effect on the device in comparison to the average rates.

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.

The performance of the Sophos XG 135W desktop device was better than most desktop 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 XG 135W meets the security needs of a network, while maintaining the performance required in a networking environment.

Copyright © 2016 Miercom

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.

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.

Copyright © 2016 Miercom