Palo Alto Networks

Next Generation Firewall (NGFW) Competitive Performance for Large Enterprise and Data Center Use Cases

Detailed Report DR210915F

Performance Validation Testing

MIERCOM.COM

CONTENTS

KEY FINDINGS

1

Business networks are a hybrid of local, remote and mobile networks that each introduce their own range of threats and vulnerabilities. Administrators need to ensure the organization, and all of its users, can safely access critical resources without affecting productivity, speed or security.

Palo Alto Networks engaged Miercom to perform independent validation testing aimed to demonstrate how deploying its security services boosts protection. Namely, with lower performance degradation than in comparable competitive solutions, resulting in a stronger security posture at a lower total cost of ownership. The PA-5450 NGFW appliance was compared to the Fortinet FortiGate FG-4201F for performance scenarios that customers can expect to experience in their networks.

Tests were run twice, once with all available services disabled ("services off") and again with all services enabled ("services on"). Real-world deployments need services enabled for optimal protection. However, customers often turn services off in order to get acceptable performance - significantly compromising security. For Palo Alto Networks, "services on" involved turning on these features and services: Threat Prevention (AV, Vulnerability Protection, Anti-spyware, File Blocking), URL Filtering, and WildFire. For Fortinet devices, "services on" involved turning on these features and services: Antivirus, Web Filter, IPS, and Application Control.

The Ixia BreakingPoint test tool with a 2x100G Cloudstorm card was used to push the limits of both the platforms for simulating large campus and data center deployments. Below are our findings.

Key Findings

- **Superior Throughput with Security Services Enabled.** Palo Alto Networks PA-5450 delivered up to 2.3x higher throughput across all parameters tested, including application traffic.
- **Superior Real-world Application Traffic Performance.** On single application tests (MySQL, SIP, and FIX), the Palo Alto Networks PA-5450 performance shows less than 1% degradation when services are enabled.
- **High Value, Low Cost of Ownership.** Palo Alto Networks PA-5450 showed higher performance compared to Fortinet FG-4201F, with 46% lower cost per protected Mbps.

It is important to note that appropriate product size is considered when deploying a NGFW appliance. Metrics for each product were observed in the intended network environment to yield the optimal, but realistic, performance. We find datasheet claims do not show results of real-world deployments, or sometimes even with security services turned on, thus giving a false impression of protection and performance capabilities. Miercom used each product as any customer would, providing objective and practical results.

Based on our observations, we found the Palo Alto Networks Next Generation Firewall PA-5450 appliance to have superior performance in multiple real-world network scenarios, with and without security features enabled. This NGFW offered superior performance to its competition, at a lower cost, making it a valuable investment for any network looking to boost security without sacrificing productivity and overhead expenses. We proudly award Palo Alto Networks the ***Miercom Performance Verified*** certification in recognition of its impressive competitive performance.

Rob Smithers

CEO, Miercom

Test Summary

2

	PA-5450	FG-4201F
Average Throughput with Services Enabled	30,703 Mbps	13,061 Mbps
TCO per Protected Mbps (A-la-carte* for Palo Alto Networks, UTP Bundle for Fortinet)	$22.20	$41.21
Throughput Comparison	PA-5450 throughput is 2.3X higher than FG-4201F	
TCO Comparison	PA-5450 TCO is 46% lower than FG-4201F	

**The license included Threat Prevention, URL Filtering, WildFire, and Premium Support for a 3 year (36 months) term.*

3 Products Tested

Palo Alto Networks PA-5450 Next Generation Firewall

This ML-powered NGFW enables granular monitoring and prevention of all threats, even for IoT environments, by classifying traffic, applications, threats, and content with robust security policies that do not burden network performance in the process. Our test system had two Data Processing Cards (DPCs) and one Networking Card (NC).

Services on:

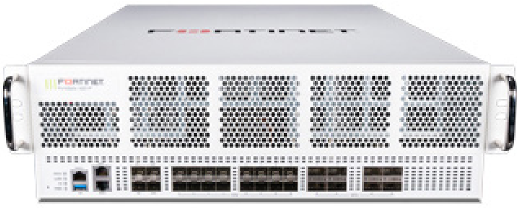
- Threat Prevention (AV, Vulnerability Protection, Anti-spyware, File Blocking)
- URL Filtering
- WildFire

PA-5450
Version 10.1.1

Fortinet FortiGate FG-4201F Network Firewall

Services on:

- Antivirus
- Web Filter
- IPS
- Application Control



FG-4201F
Version 6.2.6 build6988 (GA)

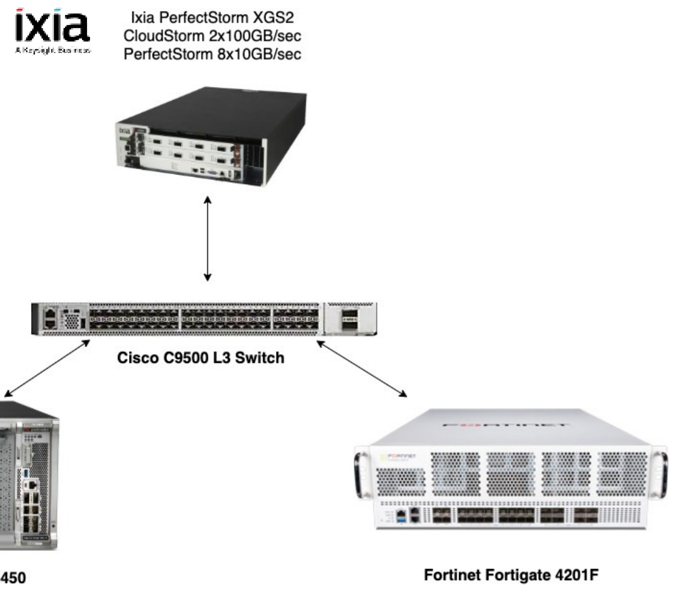
4 How We Did It

Using hands-on network testing tools, business environments were simulated and challenged with real-world traffic scenarios to provide an accurate assessment of product performance.

The Palo Alto Networks and Fortinet appliances were competitively compared using application traffic generated by Ixia CloudStorm XGS2 (v9.10.110.25) while services were disabled/enabled on the device.

All devices were configured to have security disabled ("services off") and then security enabled ("services on"). For Palo Alto Networks, "services on" involved turning on these features and services: Threat Prevention (AV, Vulnerability Protection, Anti-spyware, File Blocking), URL Filtering, and WildFire. For Fortinet devices, "services on" involved turning on these features and services: Antivirus, Web Filter, IPS, Email Filter, and Application Control.

Test Topology



Source: Palo Alto Networks

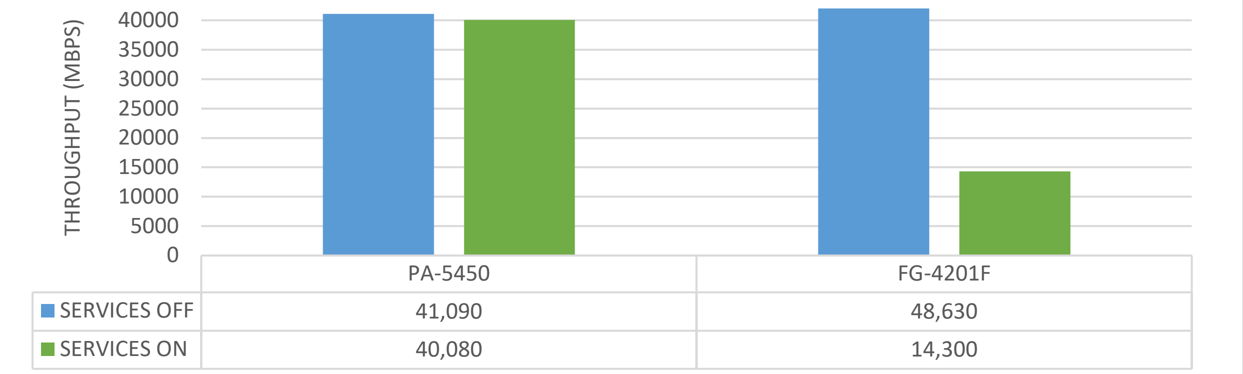
The Palo Alto PA-5450 and Fortinet FG-4201F were the Device Under Tests (DUTs) connected to the client and server sides of the Ixia Cloudstorm 100Gb/sec line card for traffic generation, testing, reporting, and packet captures. Tests began with 10,000 sessions per second, incrementing by 10,000 sessions every 5 seconds up to the maximum TCP CPS value claimed by the respective vendor.

Comparative Performance Results

5

5.1 Raw TCP Throughput with 1460-Byte Payload

Raw TCP Throughput with 1460-Byte Payload (Mbps)
Palo Alto Networks PA-5450 vs Fortinet FG-4201F



	PA-5450	FG-4201F
🟦 SERVICES OFF	41,090	48,630
🟩 SERVICES ON	40,080	14,300

Source: Miercom

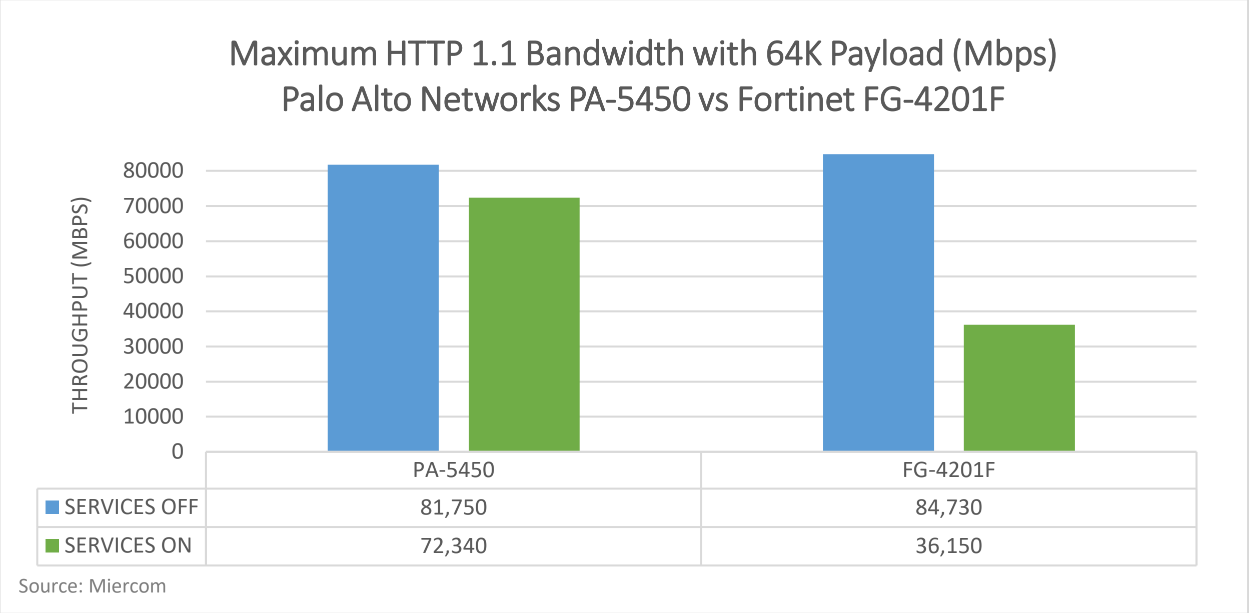
Palo Alto Networks PA-5450 degraded by just 2.5 percent, while Fortinet FG-4201F fell by 70.6 percent once services were enabled.

The Palo Alto Networks Advantage

Palo Alto Networks PA-5450 saw 2.5 percent degradation in performance with services enabled, faring much better than Fortinet which had 70.6 percent reduced performance.

5.2 Maximum HTTP 1.1 Bandwidth & Connections/sec (CPS)

5.2.1 Bandwidth with 64K Payload (Mbps)

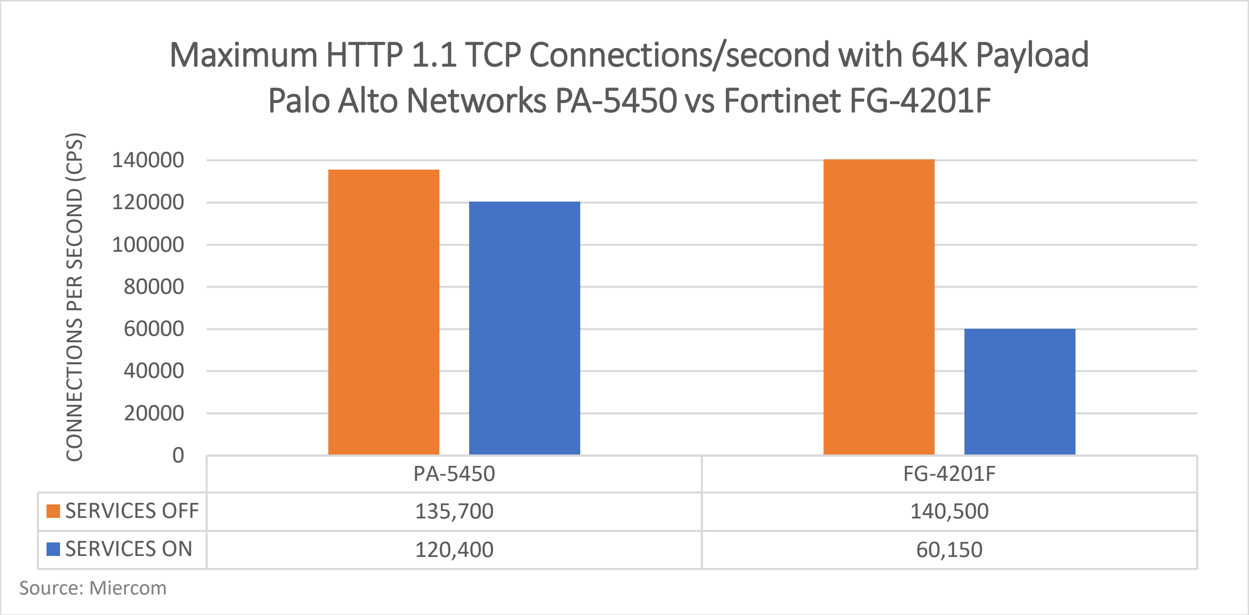


	PA-5450	FG-4201F
🟦 SERVICES OFF	81,750	84,730
🟩 SERVICES ON	72,340	36,150

Source: Miercom

For a 64K payload, Palo Alto Networks PA-5450 bandwidth degraded by 11.5 percent with services enabled, while Fortinet FG-4201F performance fell by 57.3 percent.

5.2.2 Connections/sec (CPS) with 64K Payload (Mbps)

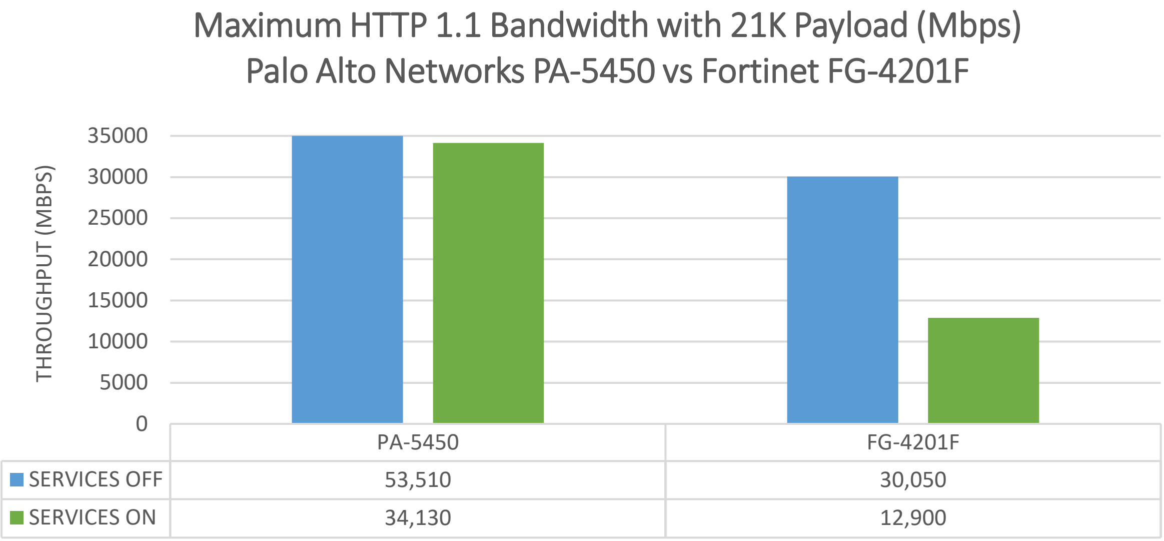


	PA-5450	FG-4201F
🟧 SERVICES OFF	135,700	140,500
🟦 SERVICES ON	120,400	60,150

Source: Miercom

For a 64K payload, Palo Alto Networks PA-5450 connection rate declined by 11.3 percent. Fortinet FG-4201F degraded by 57.2 percent.

5.2.3 Bandwidth with 21K Payload (Mbps)

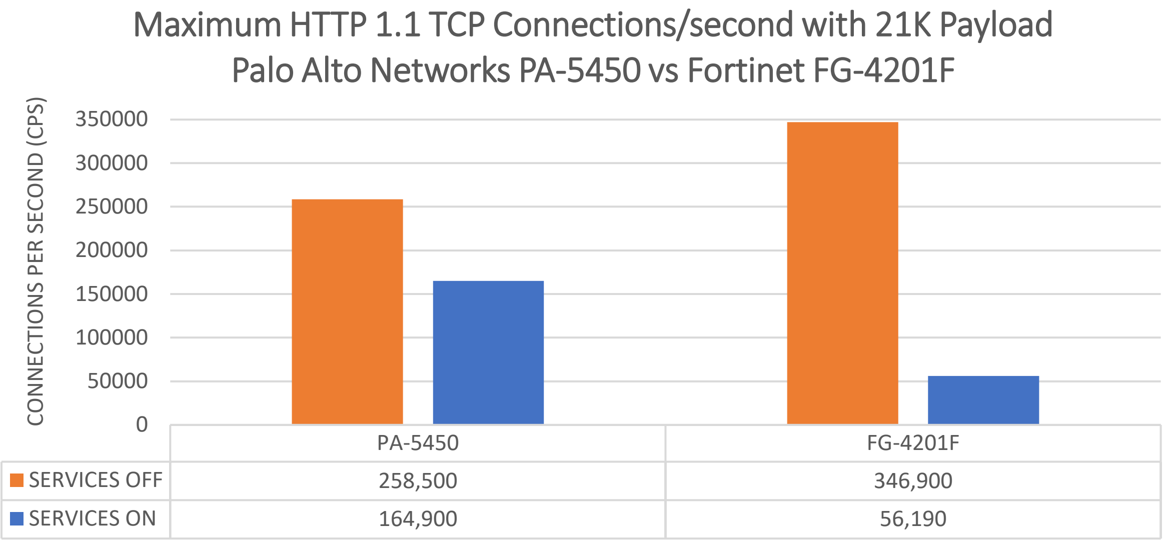


	PA-5450	FG-4201F
🟦 SERVICES OFF	53,510	30,050
🟩 SERVICES ON	34,130	12,900

Source: Miercom

For 21K payload, Palo Alto Networks PA-5450 bandwidth declined by 36.2 percent. Fortinet FG-4201F degraded by over half, at 57.3 percent.

5.2.4 Connections/sec (CPS) with 21K Payload (Mbps)



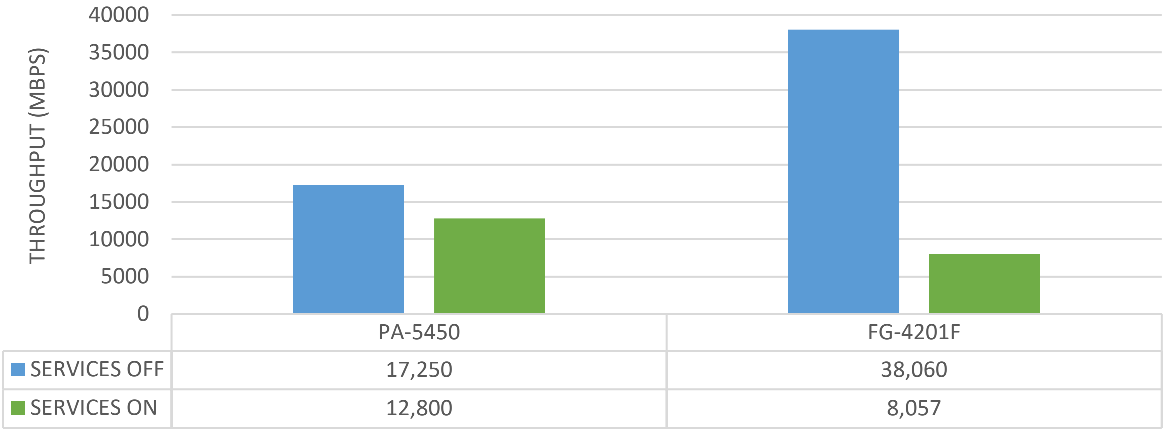
	PA-5450	FG-4201F
🟧 SERVICES OFF	258,500	346,900
🟦 SERVICES ON	164,900	56,190

Source: Miercom

For 21K payload, Palo Alto Networks PA-5450 connection rate saw degradation of 36.2 percent. Fortinet FG-4201F had significant degradation of 83.8 percent.

5.2.5 Bandwidth with 4.5K Payload (Mbps)

Maximum HTTP 1.1 Bandwidth with 4.5K Payload (Mbps)
Palo Alto Networks PA-5450 vs Fortinet FG-4201F



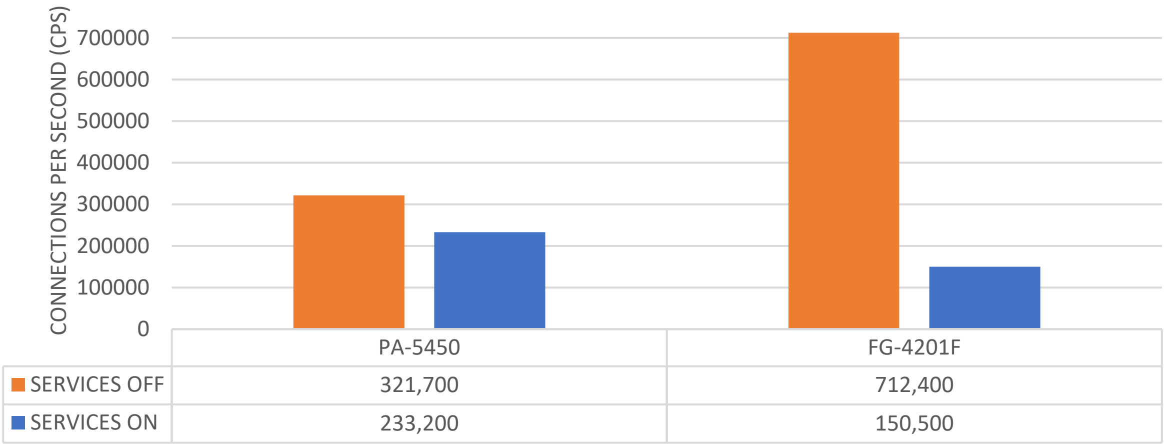
	PA-5450	FG-4201F
🟦 SERVICES OFF	17,250	38,060
🟩 SERVICES ON	12,800	8,057

Source: Miercom

For a 4.5K payload, Palo Alto Networks PA-5450 saw 25.8 percent degradation in performance when services were enabled. While initially achieving higher throughput, Fortinet FG-4201F performance dropped significantly with services enabled - by 78.8 percent.

5.2.6 Connections/sec (CPS) with 4.5K Payload (Mbps)

Maximum HTTP 1.1 TCP Connections/second with 4.5K Payload
Palo Alto Networks PA-5450 vs Fortinet FG-4201F



	PA-5450	FG-4201F
🟧 SERVICES OFF	321,700	712,400
🟦 SERVICES ON	233,200	150,500

Source: Miercom

For a 4.5K payload, Palo Alto Networks PA-5450 connection rate declined 27.5 percent when services were turned on. As with throughput, Fortinet FG-4201F had very high raw performance which dropped significantly - by 78.9 percent - once services were turned on.

The Palo Alto Networks Advantage

In this comparison of raw and security-service-enabled performance between the Palo Alto Networks PA-5450 and the Fortinet FG4201F, the Palo Alto Networks solution showed significantly lower performance degradation with security services enabled.

Bandwidth

Palo Alto Networks PA-5450 had a lower average degradation in bandwidth of 25 percent:

64K load	12 percent
21K load	36 percent
4.5K load	26 percent

Fortinet FG-4201F saw an average degradation of 64 percent:

64K load	57 percent
21K load	57 percent
4.5K load	79 percent

Connection Rate

Palo Alto Networks PA-5450 had a lower average degradation of 25 percent:

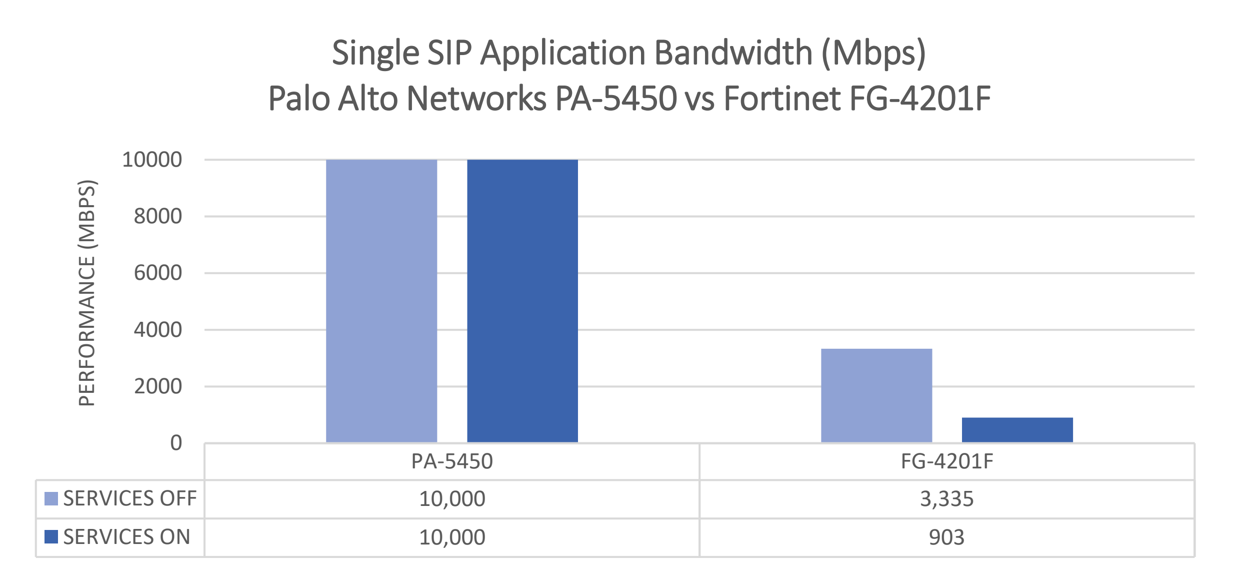
64K load	11 percent
21K load	36 percent
4.5K load	26 percent

Fortinet FG-4201F saw an average degradation of 73 percent:

64K load	57 percent
21K load	84 percent
4.5K load	79 percent

5.3 Single Application Bandwidth

5.3.1 Session Initiation Protocol (SIP) Application Bandwidth

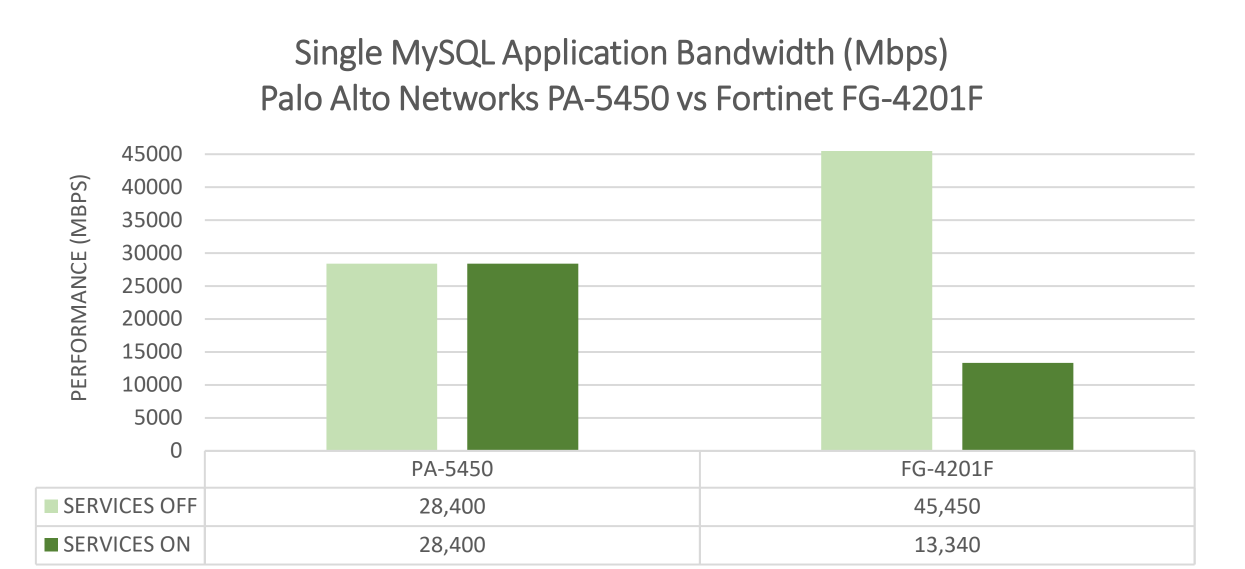


	PA-5450	FG-4201F
■ SERVICES OFF	10,000	3,335
■ SERVICES ON	10,000	903

Source: Miercom

With services enabled, Palo Alto Networks PA-5450 saw no loss in bandwidth, compared to Fortinet FG-4201F which degraded by 73 percent. Palo Alto Networks saw 3 times higher throughput than Fortinet. Once services were enabled, Palo Alto Networks had 11 times the throughput of Fortinet.

5.3.2 MySQL Application Bandwidth

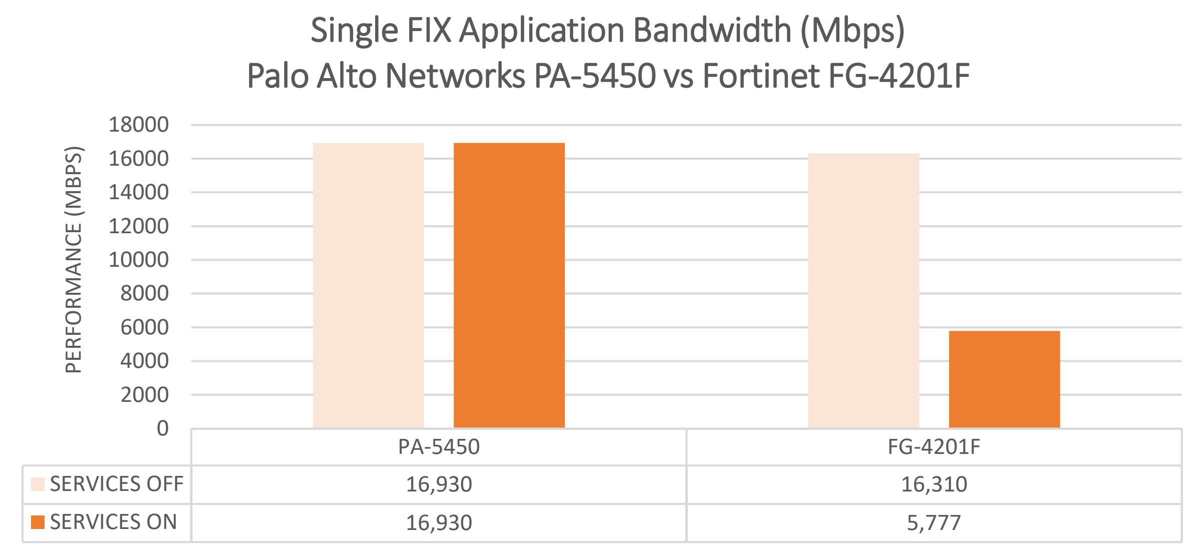


	PA-5450	FG-4201F
■ SERVICES OFF	28,400	45,450
■ SERVICES ON	28,400	13,340

Source: Miercom

With services enabled, Palo Alto Networks PA-5450 saw no change in bandwidth. Fortinet FG-4201F declined by 71 percent. When services were on, Palo Alto Networks had twice the throughput as Fortinet.

5.3.3 Financial Information eXchange (FIX) Application Bandwidth



	PA-5450	FG-4201F
▢ SERVICES OFF	16,930	16,310
■ SERVICES ON	16,930	5,777

Source: Miercom

With services enabled, Palo Alto Networks PA-5450 saw no change in bandwidth. Fortinet FG-4201F declined by 65 percent. When services were turned on, Palo Alto Networks had 3 times the throughput as Fortinet.

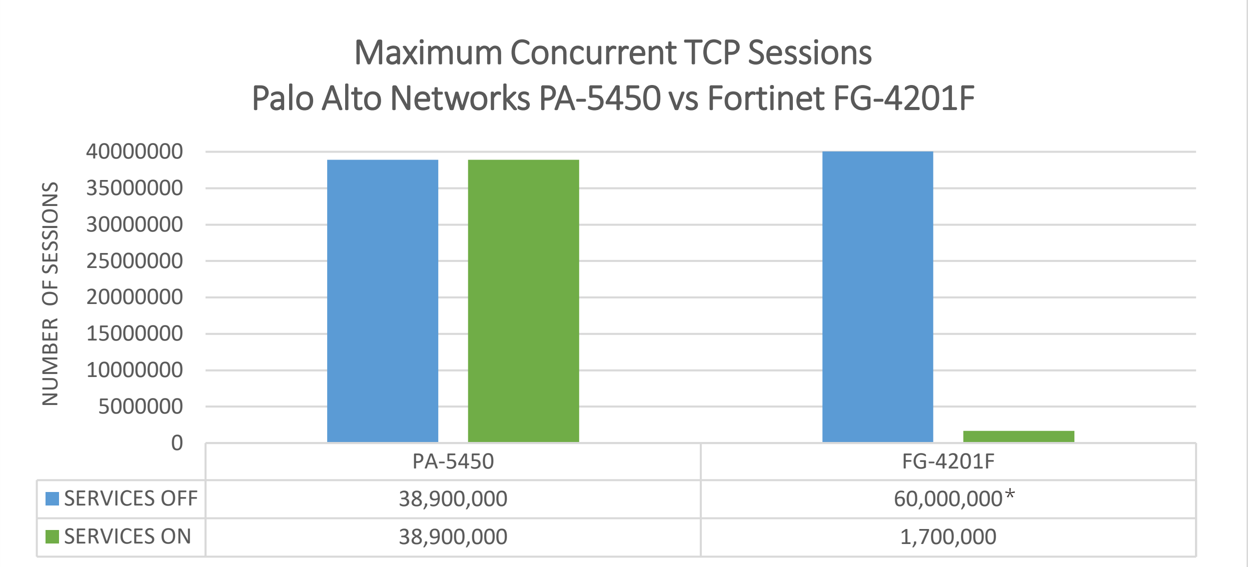
The Palo Alto Networks Advantage

Palo Alto Networks PA-5450 demonstrated less than 1 percent performance degradation for any of the following application types: SIP, MySQL, or FIX. It delivered up to 11 times the throughput compared to the Fortinet FG-4201F when security services were enabled.

Fortinet FG-4201F dropped by 73 percent for SIP, 71 percent for MySQL, and 65 percent for FIX applications.

5.4 TCP Maximum Capacity

5.4.1 Maximum Concurrent TCP Sessions



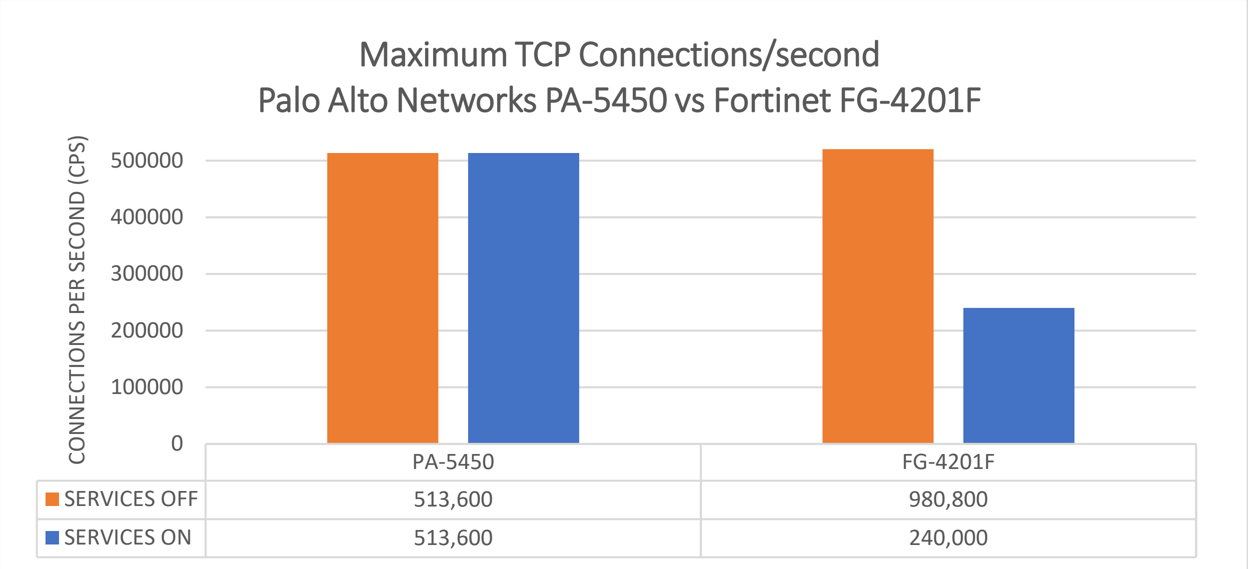
	PA-5450	FG-4201F
🟦 SERVICES OFF	38,900,000	60,000,000*
🟩 SERVICES ON	38,900,000	1,700,000

Source: Miercom

Once services were enabled, Palo Alto Networks PA-5450 saw no change in throughput. Fortinet FG-4201F significantly declined by over 97 percent. Palo Alto Networks provided up to 23 times higher throughput than Fortinet.

*Note: The Ixia BreakingPoint module was scalable only up to 60 million sessions. The FG-4201F could have achieved higher session count than the capacity of the test tool used.

5.4.2 Maximum TCP Connections/sec (CPS)



	PA-5450	FG-4201F
🟧 SERVICES OFF	513,600	980,800
🟦 SERVICES ON	513,600	240,000

Source: Miercom

Once services were enabled, Palo Alto Networks PA-5450 saw no change in connection rate. Fortinet FG-4201F significantly declined by 76 percent. Palo Alto Networks provided twice the connection rate as Fortinet.

The Palo Alto Networks Advantage

Palo Alto Networks PA-5450 had no change in capacity for concurrent TCP sessions once services were enabled. Fortinet FG-4201F had significant degradation of 97 percent.

For connection rate, Palo Alto Networks experienced no change; Fortinet saw 76 percent degradation.

Total Cost of Ownership

6

As with performance testing, we compared NGFW products for their performance and cost-benefit value in Cost per Mbps (USD). We evaluated the average throughput (in Mbps) and total cost of acquisition (hardware, subscription and support pricing). The following tables and charts provide details on the total Cost/Mbps calculations.

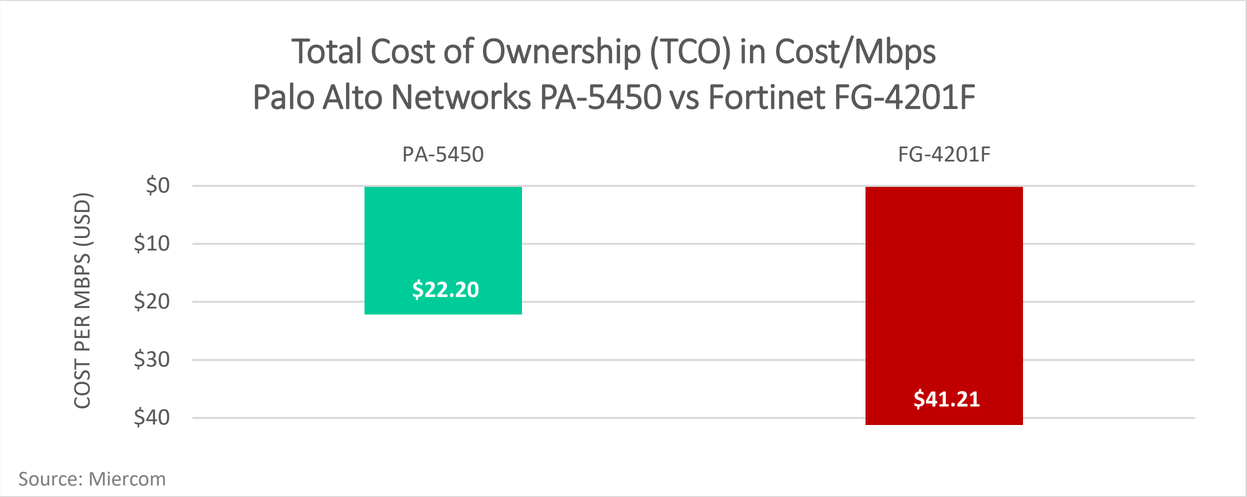
TCO Calculations

Product	Average Throughput (Mbps)	Total Cost (USD)	Hardware Cost (USD)	Subscription & Support Cost (USD)	Cost/Mbps
PA-5450	30,702.86	***$681,670***	$246,190	$435,480	***$22.20***
FG-4201F	13,061.00	***$538,183***	$182,435	$355,748	***$41.21***

Comparative Price and TCO Calculations: Palo Alto Networks vs Fortinet

Product Comparison	Price Difference (Hardware and Subscriptions)	TCO per Protected Mbps DIfference
PA-5450 vs FG-4201F	***+27.0%***	***-46%***

Note: The the total costs of acquisition are based on prices as of July 1, 2021.



Source: Miercom

Palo Alto Networks PA-5450 offers an 46 percent cost savings per Mbps when compared to the Fortinet FG-4201F appliance, which has a substantially higher cost of about $41 per Mbps. While Fortinet may cost less in hardware, subscriptions and support, they provide less than half the performance.

About Miercom Performance Verified

This report was sponsored by Palo Alto Networks. The data was obtained completely and independently by Miercom engineers and lab-test staff as part of our Performance Verified assessment. Testing such as this is based on a methodology that is jointly co-developed with the sponsoring vendor. The test cases are designed to focus on specific claims of the sponsoring vendor, and either validate or repudiate those claims. The results are presented in a report such as this one, independently published by 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; Miercom 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.

By downloading, circulating or using this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Security Services

Palo Alto Networks offers the following security services.

- **Threat Prevention:** Goes beyond traditional intrusion prevention system (IPS) to prevent all known threats across all traffic in a single pass without sacrificing performance
- **URL Filtering:** Provides best in class web protection while maximizing operational efficiency with the industry's first real-time web protection engine and industry-leading phishing protections
- **Wildfire:** Ensures files are safe with automatic detection and prevention of unknown malware powered by industry-leading cloud-based analysis and crowd-sourced intelligence from over 42,000 customers
- **DNS Security:** Harnesses the power of machine learning to detect and prevent threats over DNS in real-time and empowers security personnel with the intelligence and context to craft policies and respond to threats quickly and effectively.
- **IoT Security:** Provides the industry's most comprehensive IoT Security solution delivering ML-powered visibility, prevention, and enforcement in a single platform
- **Enterprise DLP:** The industry's first cloud-delivered enterprise DLP that consistently protects sensitive data across networks, clouds, and users
- **SaaS Security:** Delivers integrated SaaS Security, that lets you see and secure new SaaS applications, protect data and prevent zero day threats at the lowest TCO.

Test Results

Test	PA-5450			FG-4201F		
	Services off	Services on	Degredation (%)	Services off	Services on	Degredation (%)
5.1 Raw TCP Throughput with 1460-Byte Payload (Mbps)						
	41,090	40,080	2.46%	48,630	14,300	70.6%
5.2 Maximum HTTP 1.1 Connections/sec (CPS) and Bandwidth (Mbps) with 64/21/4.5K Payload						
64K BW	81,750	72,340	11.5%	84,730	36,150	57.3%
64K CPS	135,700	120,400	11.3%	140,500	60,150	57.2%
21K BW	53,510	34,130	36.2%	30,050	12,900	57.1%
21K CPS	258,500	164,900	36.2%	346,900	56,190	83.8%
4.5K BW	17,250	12,800	25.8%	38,060	8,057	78.3%
4.5K CPS	321,700	233,200	27.5%	712,400	150,500	78.9%
5.3 Single Application Performance (Mbps) before "Application Transaction Failures" exceed 20						
SIP	10,000	10,000	0.0%	3,335	903	72.9%
MySQL	28,400	28,400	0.0%	45,450	13,340	70.7%
FIX	16,930	16,930	0.0%	16,310	5,777	64.6%
5.4 Maximum TCP Capacity Concurrent TCP Sessions and Connections/sec (CPS)						
Max Conc. Sessions	39.8 M	39.8 M	0.0%	60.0 M	1.7 M	97.2%
Max CPS	513.6 K	513.6 K	0.0%	980.8 K	240 K	75.5%