# Palo Alto Networks

## Next Generation Firewall (NGFW) Competitive Performance for Enterprise HQ and Data Center Edge Use Cases

**27 July 2022**

**Detailed Report DR220527E**

Performance Validation Testing

MIERCOM.COM

# CONTENTS

# KEY FINDINGS

1

Network administrators need to secure and protect networks from threats originating at the Internet edge, as well as threats that have embedded in network traffic traversing the network. Administrators need to ensure the organization, and all of its users can safely access critical resources without affecting productivity, speed or security.

By engaging Miercom to perform independent validation testing, Palo Alto Networks aimed to prove how deploying its security services on the firewalls can boost protection without degrading performance. The PA-3420, PA-3440, and PA-5430 NGFW appliances were compared to the Fortinet FortiGate (FG) FG-1801F, FG-2601F, and 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, Data Filtering, File Blocking), Advanced URL Filtering, DNS Security, and WildFire. For Fortinet devices, "services on" involved turning on these features and services: Antivirus, Web Filter, IPS, File Filter, and Email Filter.

The Ixia BreakingPoint PerfectStorm test tool was used to push the limits of each competing platform, utilizing an 8x10-GE line card, for different scenarios commonly seen in Enterprise HQ and Data Center environments. Devices were compared for single port-pair performance for a realistic and consistent test.

Below are our findings.

## Key Findings

- **Superior Throughput with Security Services Enabled.** Palo Alto Networks saw up to 1.3x higher throughput across all parameters tested, including application traffic.
- **Superior Real-world Application Traffic Performance.** On services enabled for single application tests (MSSQL, SIP, FIX and RDP), the Palo Alto Networks performance shows consistently low degradation, with an average of 9.7%, and up to 64 percent better average throughput.
- **Higher Value, Lower Cost of Ownership.** Palo Alto Networks showed higher performance with security services enabled and lower cost for every appliance compared to similar Fortinet products, with cost per 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.

To achieve comprehensive network security, network security administrators expect to be able to deploy security services on the NGFW with minimal degradation of NGFW performance. Based on our observations, we found the Palo Alto Networks Next Generation Firewall PA-3420/3440/5430 appliances to have superior performance in multiple real-world network scenarios, with and without security features enabled. Enterprises need to provide consistent security across their networks, but doing so usually degrades performance. However, this series outperformed 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-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| Average Throughput with Services Enabled (Mbps) | 2,911.10 | 2,262.36 | 4,128.61 | 3,995.83 | 9,179.84 | 9,146.08 |
| TCO per Protected Mbps (Pro-Bundle for Palo Alto Networks, UTP Bundle for Fortinet) | $51.71 | $65.24 | $53.86 | $54.53 | $66.80 | $72.49 |
| Throughput Comparison | PA-3420 throughput is 1.29X better than FG-1801F | | PA-3440 throughput is better than FG-2601F | | PA-5430 throughput is better than FG-2601F | |
| TCO Comparison | PA-3420 TCO is 1.26X better than FG-1801F | | PA-3440 TCO is better than FG-2601F | | PA-5430 TCO is 1.1X better than FG-4201F | |

# 3 Products Tested

## Palo Alto Networks PA-3420/3440/5430 Next Generation Firewall

These new additions to Palo Alto Networks' NGFW portfolio allow customers to deploy devices for retail, commercial locations, and managed services deployments. Testing for the following products focused on small business (SMB) and data center/service provider use cases.

**Security Services:**
- Threat Prevention (AV, Vulnerability Protection, Anti-spyware, Data Filtering, File Blocking)
- Advanced URL Filtering
- DNS Security
- WildFire

**PA-3420**
Version 10.2.0 GA

**PA-3440**
Version 10.2.0 GA

**PA-5430**
Version 10.2.1 GA

## Fortinet FortiGate FG-1801F/2601F/4201F Network Firewall

**Security Services:**
- Antivirus
- Web Filter
- IPS
- File Filter
- Email Filter

**FG-1801F**
Version 7.0.5 build 304
(flow mode)

**FG-2601F**
Version 7.0.5 build 304

**FG-4201F**
Version 6.4.9 build 1966

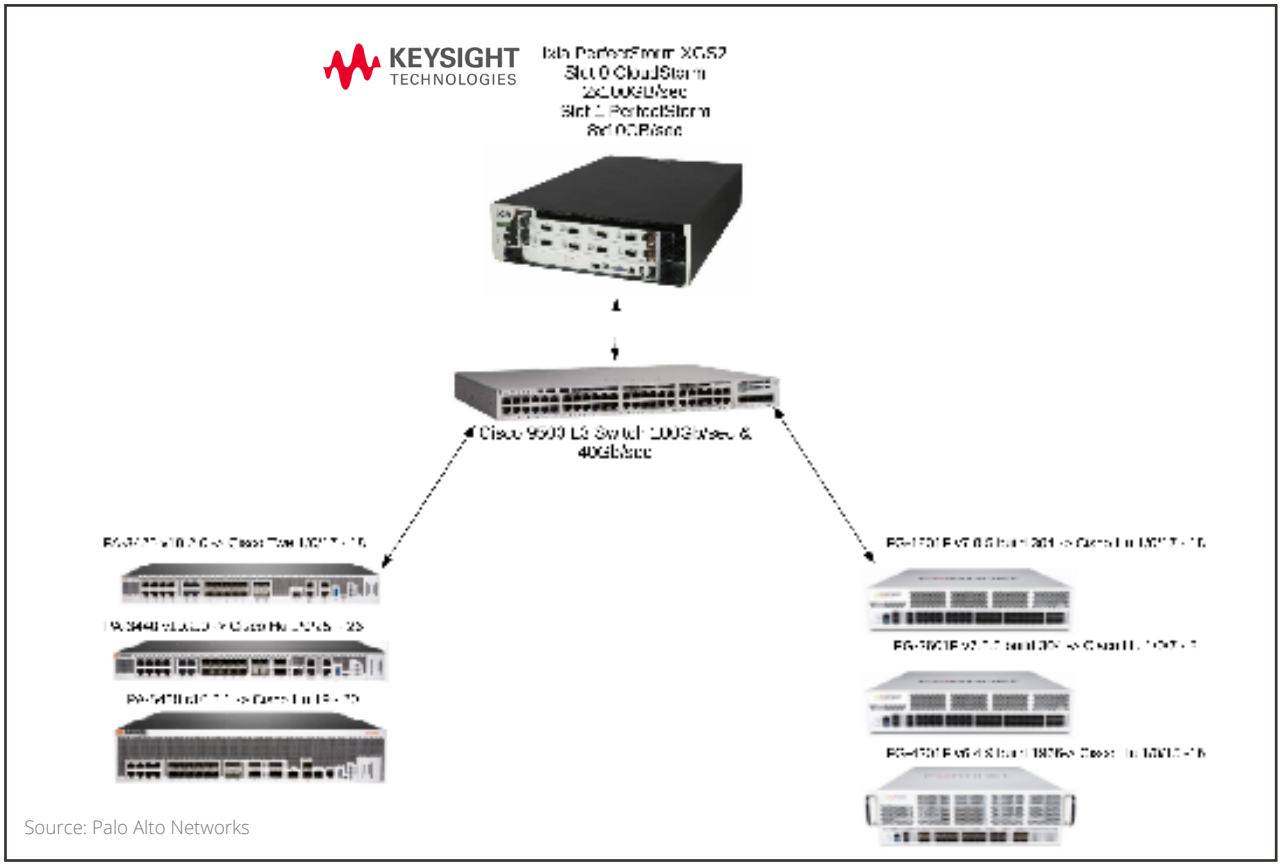
# 4 How We Did It

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 Keysight (Ixia) PerfectStorm XGS2 (v9.20.15.12) 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, Data Filtering, File Blocking), Advanced URL Filtering, DNS Security, and WildFire. For Fortinet devices, "services on" involved turning on these features and services: Antivirus, Web Filter, IPS, File Filter, and Email Filter.

## 4.1 Test Topology




Source: Palo Alto Networks

*The Palo Alto PA-3420/3440/5430 and Fortinet FG-1801F/2601F/4201F were the Device Under Tests (DUTs) connected via a single port pair to the client and server sides of the Keysight (Ixia) XGS2 CloudStorm 2x100-GE line card and PerfectStorm 8x10-GE line card for traffic generation, testing, reporting, and packet captures. Tests began with 1,000 sessions and incremented by 1,000 sessions every 10 seconds.*

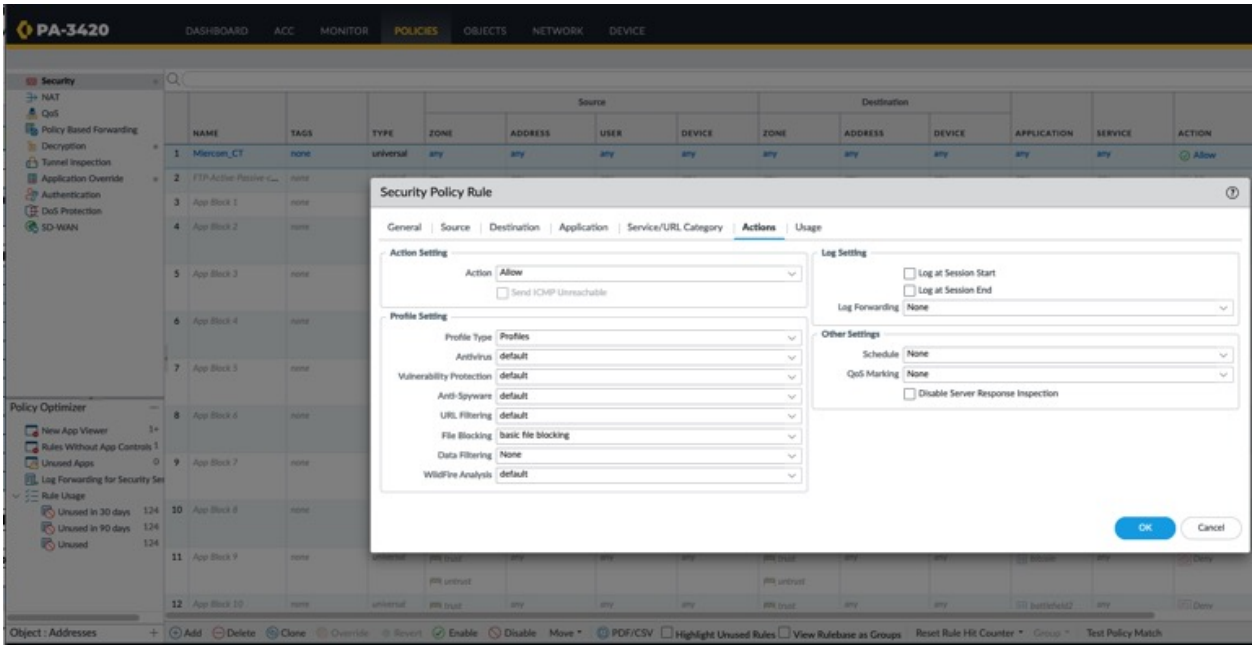
## 4.3 Device Configurations

All devices under test are tested with all security services on and all security services off. While the nomenclature for the device security features vary, the offerings are equivalent in actual functionality.

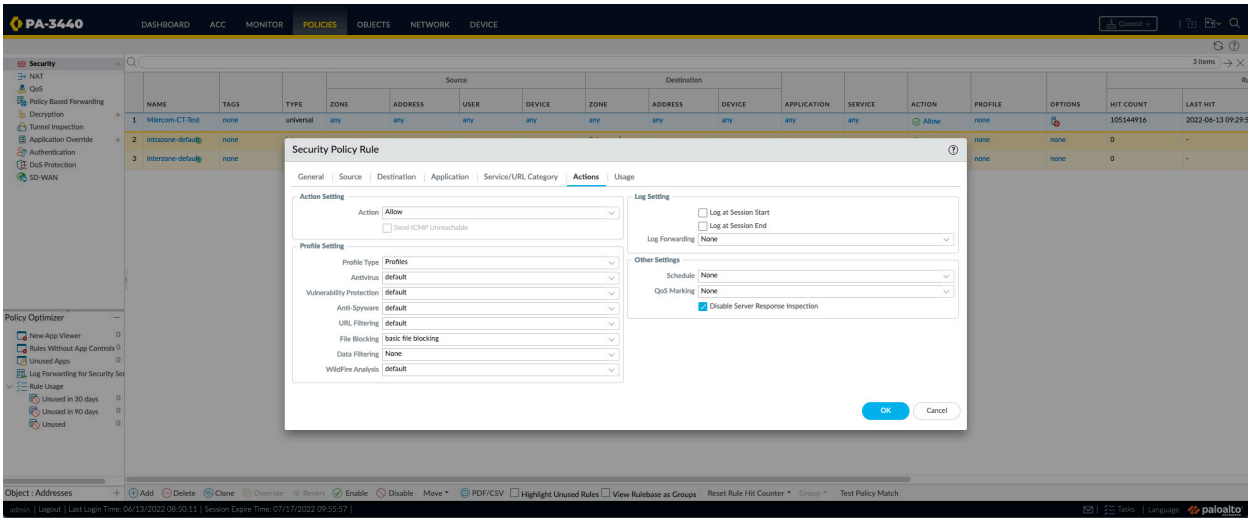
### 4.3.1 Palo Alto Networks Configurations

The following images depict the security policy configurations for the PA-3420/3420/5430 appliances.

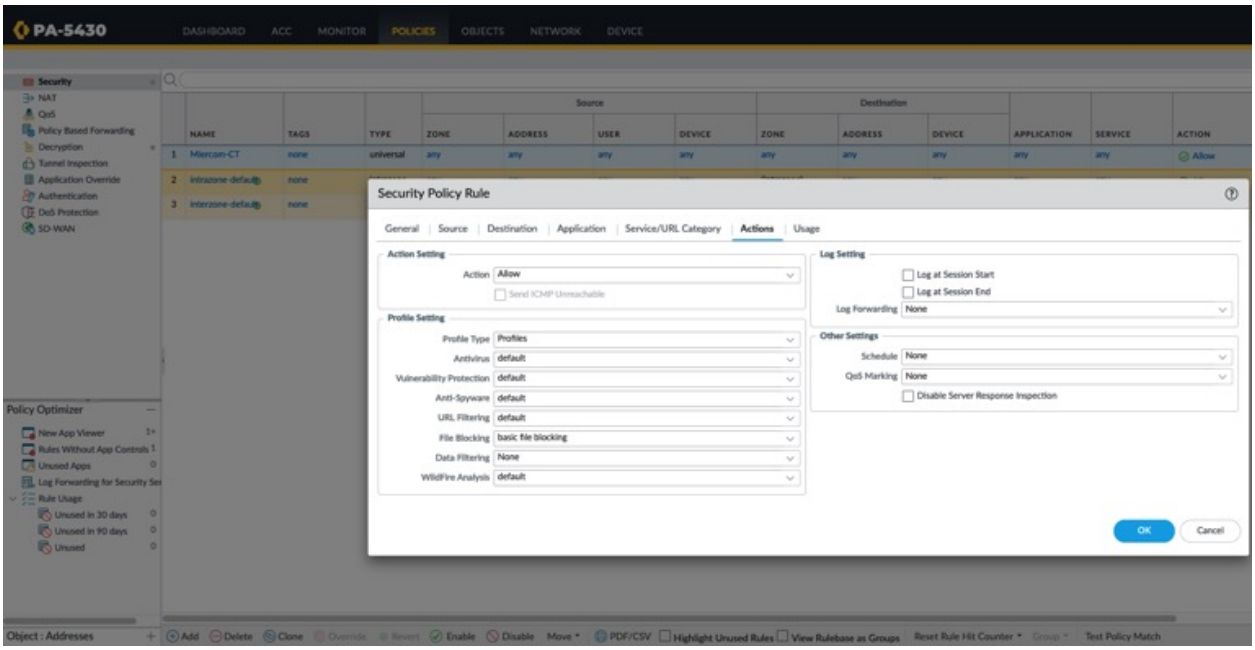
**PA-3420:**




**PA-3440:**



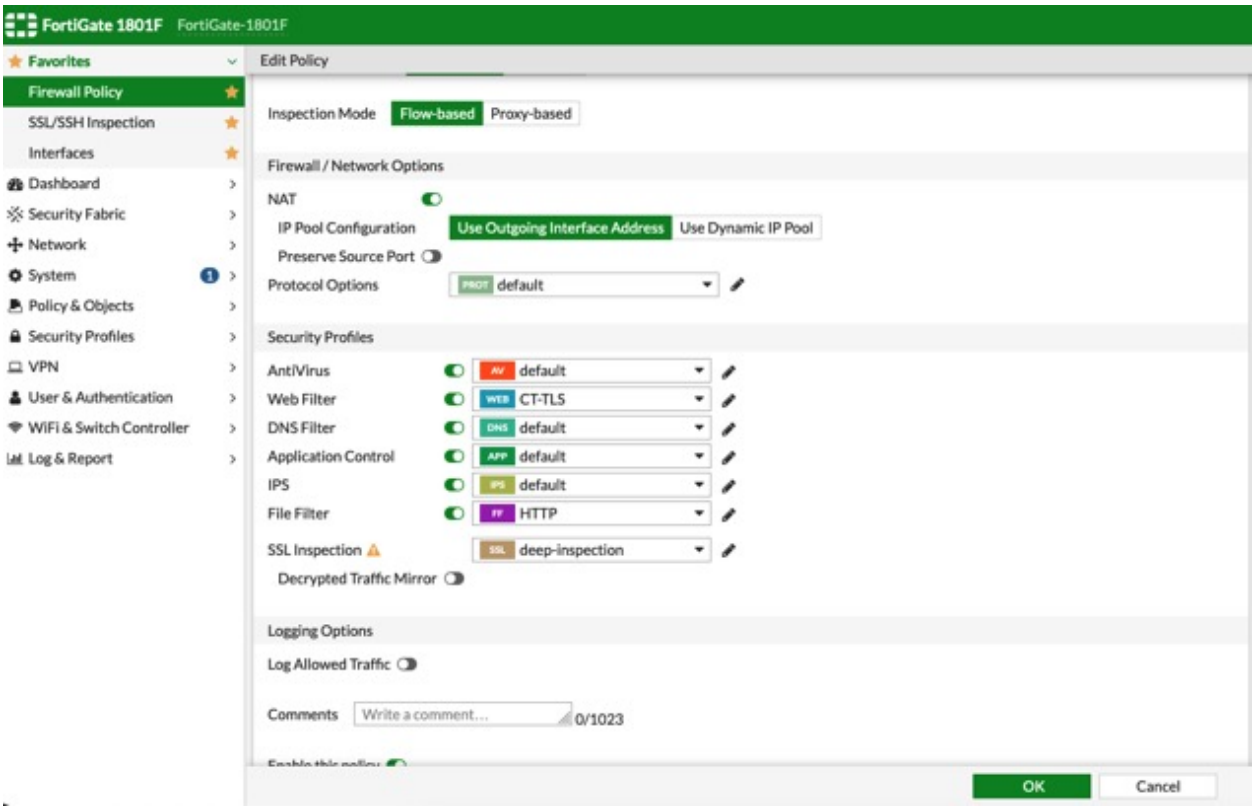
### PA-5430:



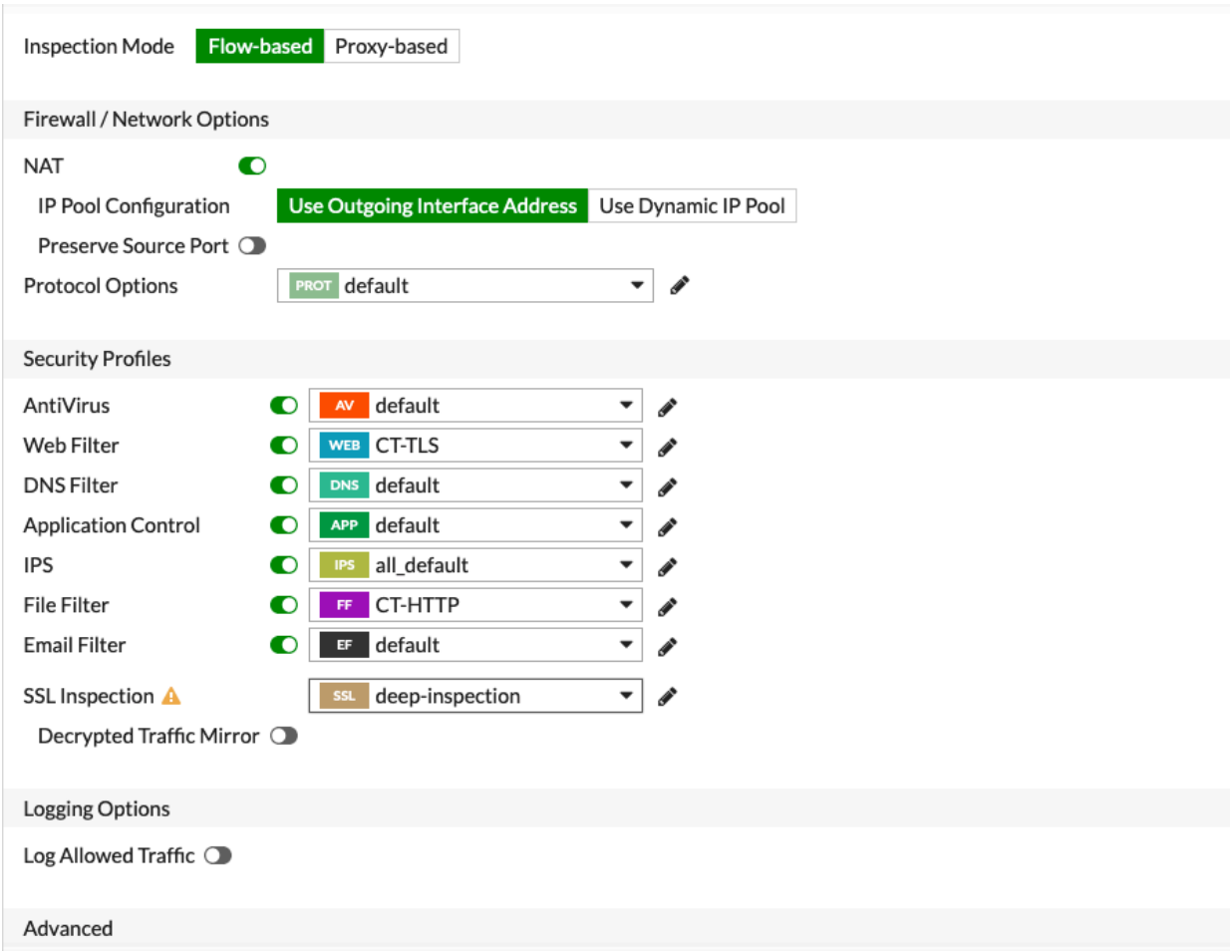

## 4.3.2 Fortinet FortiGate Configurations

The following images depict the security policy configurations for the FG-1801F/2601F/4201F appliances.

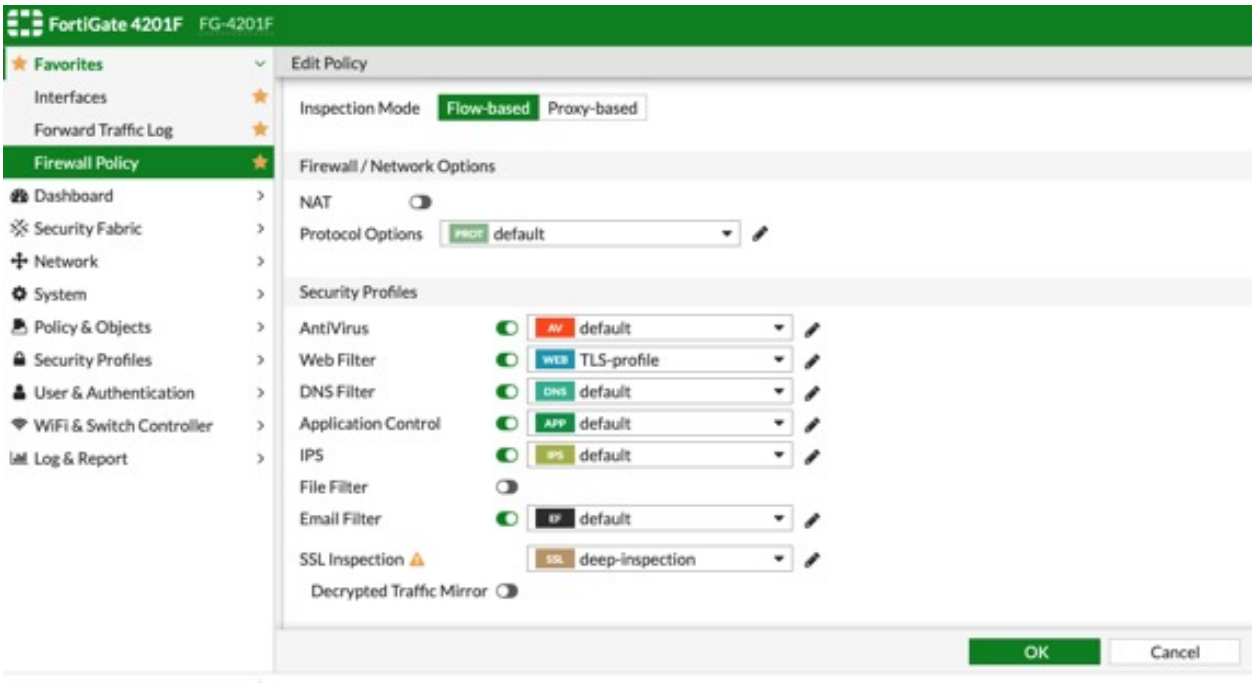
### FG-1801F:



## FG-2601F:




## FG-4201F:

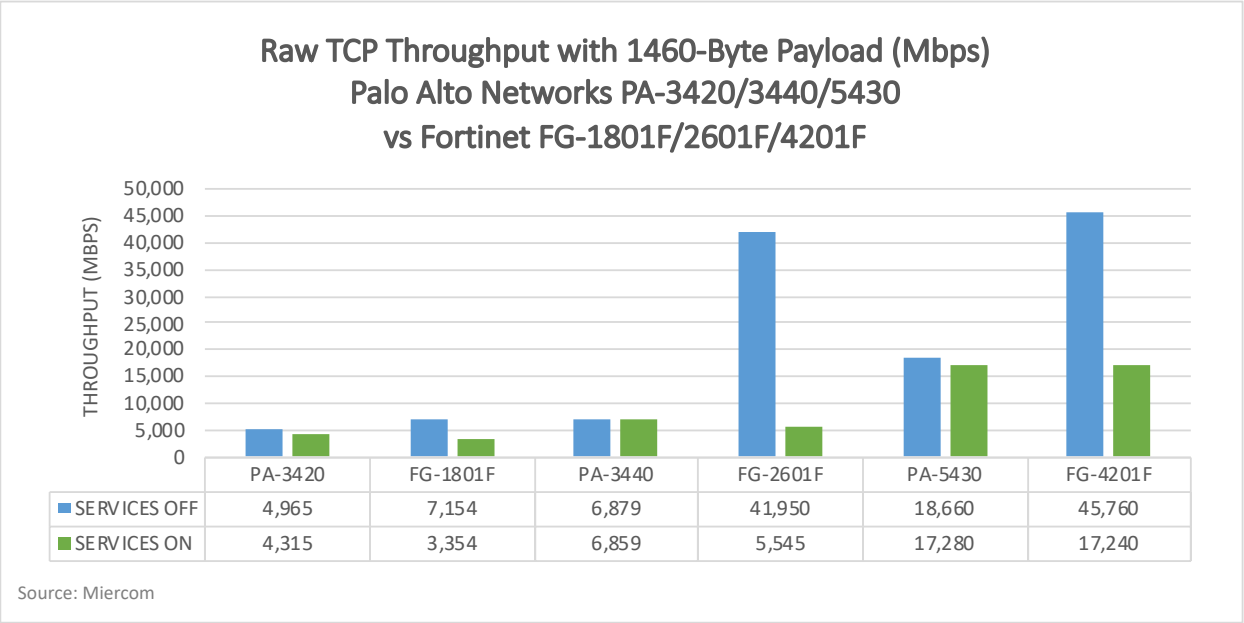


# Comparative Performance Results

5

## 5.1 Raw TCP Throughput with 1460-Byte Payload

This test measured the maximum achievable bandwidth, utilizing a 1460-byte payload. We recorded bandwidth, with security services enabled and disabled.




| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 4,965 | 7,154 | 6,879 | 41,950 | 18,660 | 45,760 |
| SERVICES ON | 4,315 | 3,354 | 6,859 | 5,545 | 17,280 | 17,240 |

Source: Miercom

*Palo Alto Networks PA-3420 degraded by just 13 percent, while Fortinet FG-1801F fell by 53 percent once services were enabled. PA-3440 saw negligible degradation of 0.29 percent with services enabled, but Fortinet FG-2601F performance dropped by 87 percent. PA-5430 degraded by 7.4 percent compared to Fortinet FG-4201F performance falling by more than 62 percent.*

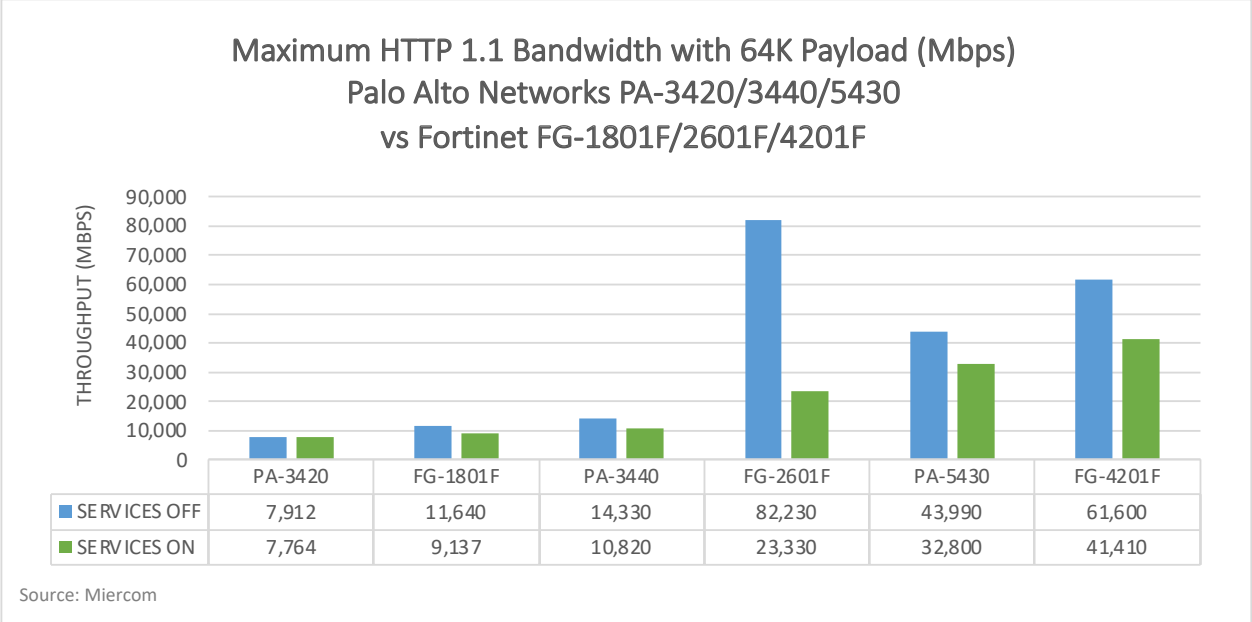
## The Palo Alto Networks Advantage

For all Palo Alto Networks appliances, Palo Alto Networks saw an average of just 6.9 percent degradation in performance with services enabled, faring much better than Fortinet which had an average of 67 percent reduced performance.

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

This test evaluated various payload sizes of 4.5KB, 21KB, 64KB in response to an HTTP 1.1 GET Request. We recorded bandwidth and TCP connections/second, with security services enabled and disabled. Tests were considered failed once TCP concurrent sessions showed exponential increase and/or application transaction failure exceeding 1% of the overall application transaction attempts.

### 5.2.1 Bandwidth with 64K Payload (Mbps)

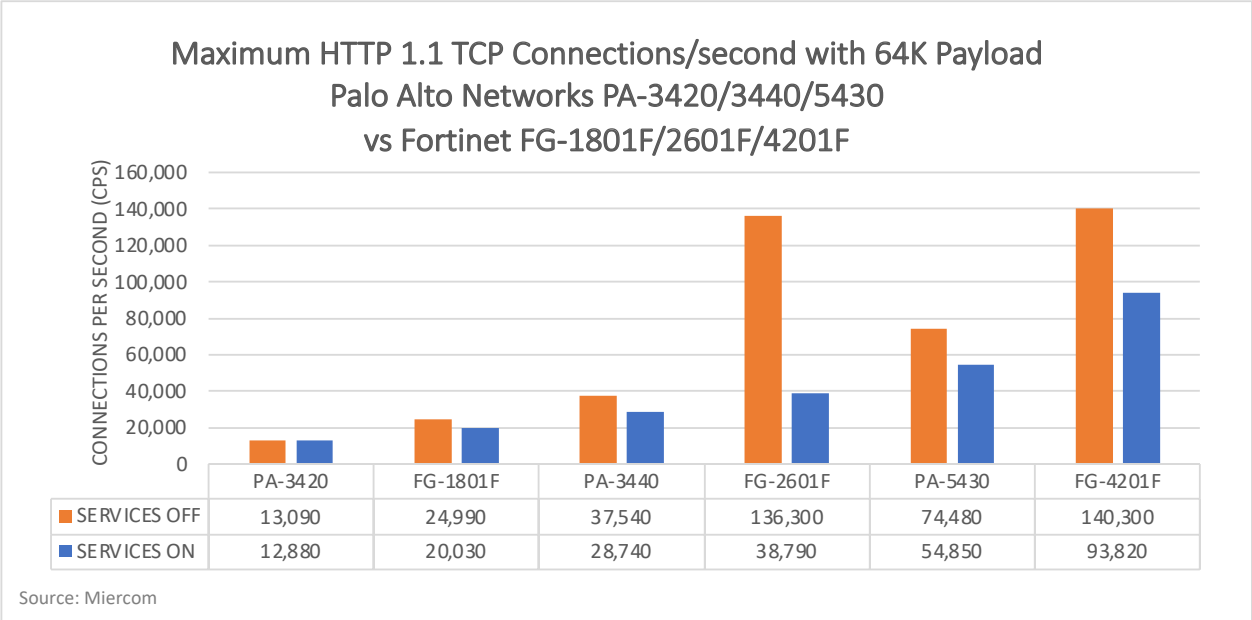



| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 7,912 | 11,640 | 14,330 | 82,230 | 43,990 | 61,600 |
| SERVICES ON | 7,764 | 9,137 | 10,820 | 23,330 | 32,800 | 41,410 |

Source: Miercom

*For a 64K payload, Palo Alto Networks PA-3420 degraded by 1.9 percent with services enabled, while Fortinet FG-1801F performance fell by 22 percent. PA-3440 saw 25 percent degradation; FG-2601F performance dropped by 72 percent. PA-5430 saw 25 percent degradation, while FG-4201F dropped by 33 percent.*

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

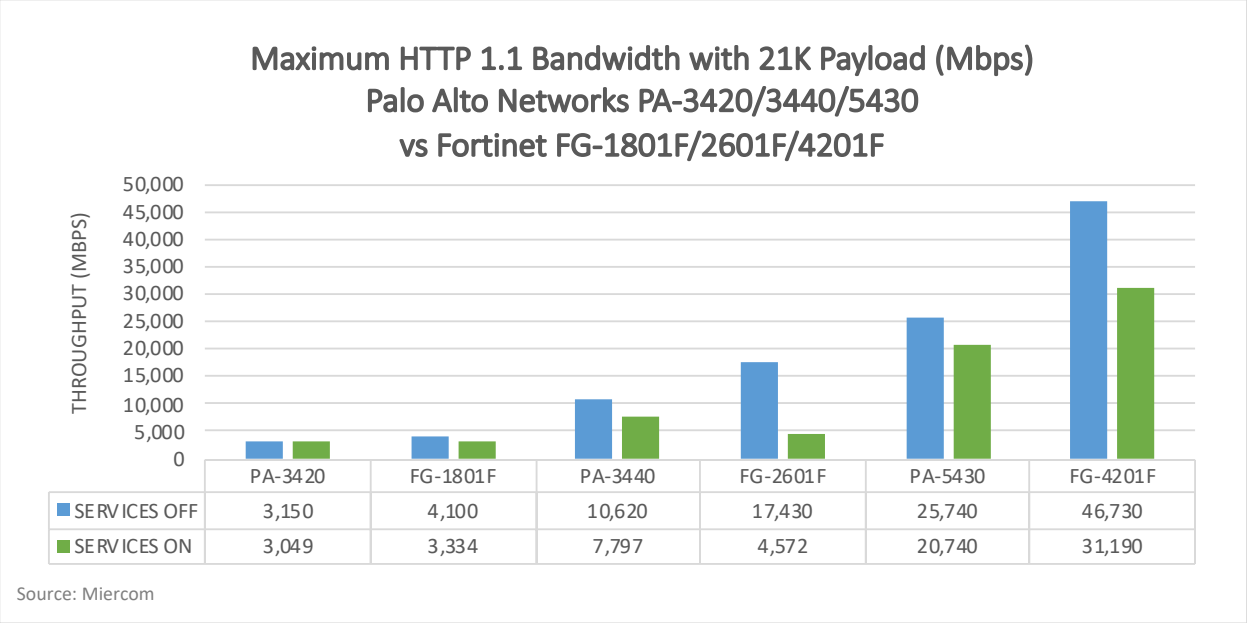



| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 13,090 | 24,990 | 37,540 | 136,300 | 74,480 | 140,300 |
| SERVICES ON | 12,880 | 20,030 | 28,740 | 38,790 | 54,850 | 93,820 |

Source: Miercom

*For a 64K payload, Palo Alto Networks PA-3420 connection rate saw little degradation of 1.6 percent when services were enabled, with Fortinet FG-1801F degrading by 20 percent. PA-3440 saw 23 percent drop in connection rate, while FG-2601F fell by 72 percent. PA-5430 degraded by 26 percent, with Fortinet FG-4201F reduced by 33 percent.*

### 5.2.3 Bandwidth with 21K Payload (Mbps)

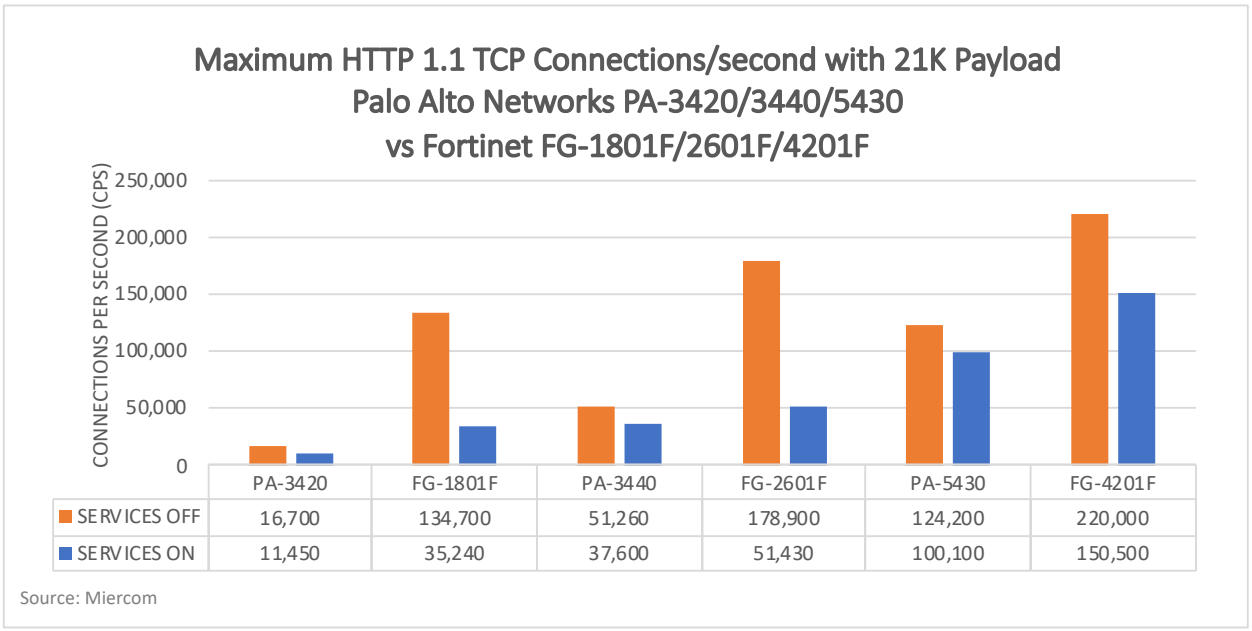



| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 3,150 | 4,100 | 10,620 | 17,430 | 25,740 | 46,730 |
| SERVICES ON | 3,049 | 3,334 | 7,797 | 4,572 | 20,740 | 31,190 |

Source: Miercom

*For 21K payload, Palo Alto Networks PA-3420 bandwidth declined by a low 3.2 percent once services were enabled, with Fortinet FG-1801F having a loss of 19 percent. PA-3440 degraded by 27 percent, compared to the 74 percent loss seen by FG-2601F. PA-5430 barely fell by 19 percent, while FG-4201F bandwidth decreased by 33 percent.*

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

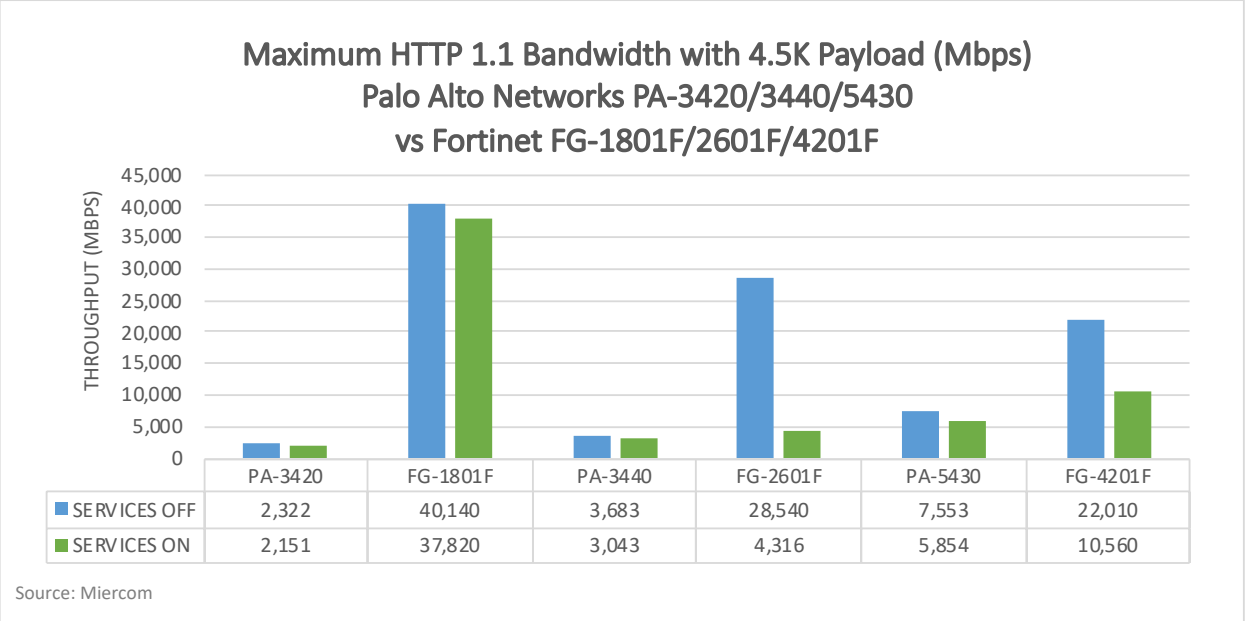



| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 16,700 | 134,700 | 51,260 | 178,900 | 124,200 | 220,000 |
| SERVICES ON | 11,450 | 35,240 | 37,600 | 51,430 | 100,100 | 150,500 |

Source: Miercom

*For 21K payload, Palo Alto Networks PA-3420 connection rate saw little degradation of 32 percent once services were enabled, compared to Fortinet FG-1801F falling 74 percent. PA-3440 connection rate dropped by 27 percent, while Fortinet FG-2601F fell by 71 percent. PA-5430 connection rate degraded by 19 percent, unlike Fortinet FG-4201F which fell by 32 percent.*

### 5.2.5 Bandwidth with 4.5K Payload (Mbps)

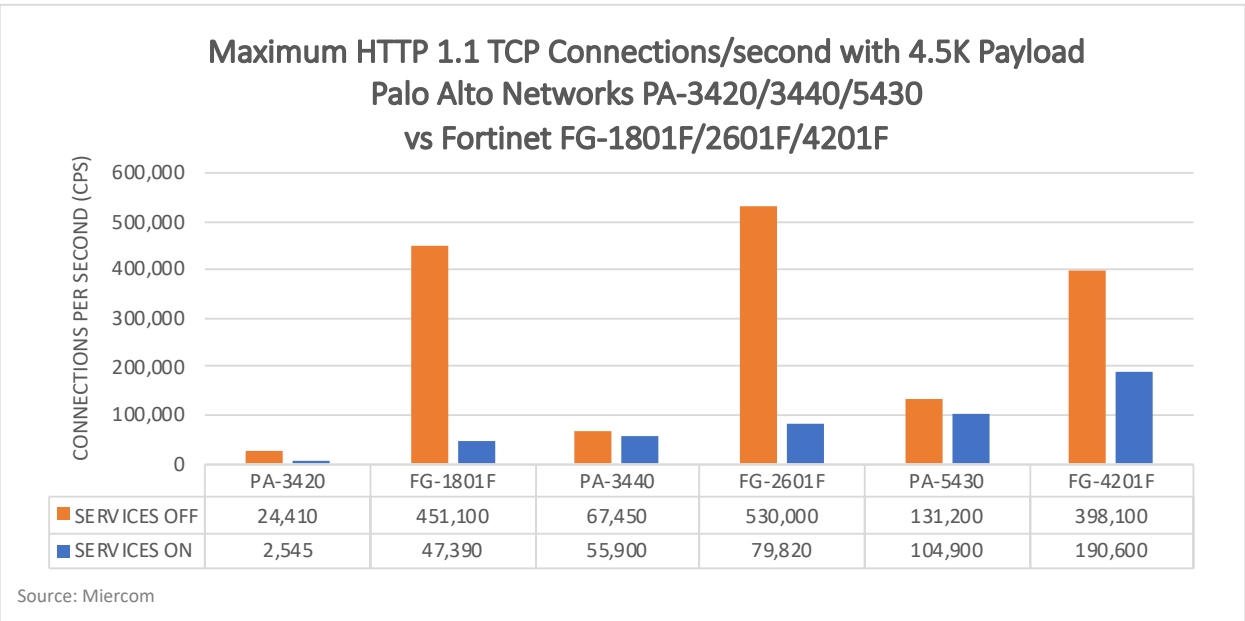



| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 2,322 | 40,140 | 3,683 | 28,540 | 7,553 | 22,010 |
| SERVICES ON | 2,151 | 37,820 | 3,043 | 4,316 | 5,854 | 10,560 |

Source: Miercom

*For a 4.5K payload, Palo Alto Networks PA-3420 bandwidth declined by 7.4 percent with services turned on; Fortinet FG-1801F saw loss of 5.8 percent. PA-3440 saw 17.4 percent degradation, whereas FG-2601F dropped by 85 percent. PA-5430 bandwidth degraded by 23 percent, compared to FG-4201F decreasing by 52 percent.*

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




| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 24,410 | 451,100 | 67,450 | 530,000 | 131,200 | 398,100 |
| SERVICES ON | 2,545 | 47,390 | 55,900 | 79,820 | 104,900 | 190,600 |

Source: Miercom

*For a 4.5K payload, both Palo Alto Networks PA-3420 and FG-1801F connection rate declined by 90 percent with services turned on. PA-3440 saw 17 percent decreased connection rate when services were enabled, but FG-2601F degraded by 85 percent. PA-5430 connection rate degraded by 20 percent, compared with FG-4201F dropping by more than 52 percent.*

## The Palo Alto Networks Advantage

Palo Alto Networks saw much less degradation than Fortinet once services were enabled - regardless of payload size. On average, Palo Alto Networks never saw degradation of more than 18 percent, with services enabled; Fortinet's degradation reached as high as 48 percent.

### 64K Payload

For bandwidth, Palo Alto Networks performance degraded by an average of 17 percent when services were enabled. Fortinet had an average 42 percent loss in bandwidth. For connection rate, Palo Alto Networks decreased by an average of 17 percent. Fortinet's average rate fell by 42 percent.

### 21K Payload

For bandwidth, Palo Alto Networks maintained sufficient performance when services were enabled - falling by 16 percent on average. Fortinet had an average 42 percent loss in bandwidth. For connection rate, Palo Alto Networks saw 26 percent average degradation. Fortinet appliances fell by an average of 59 percent.

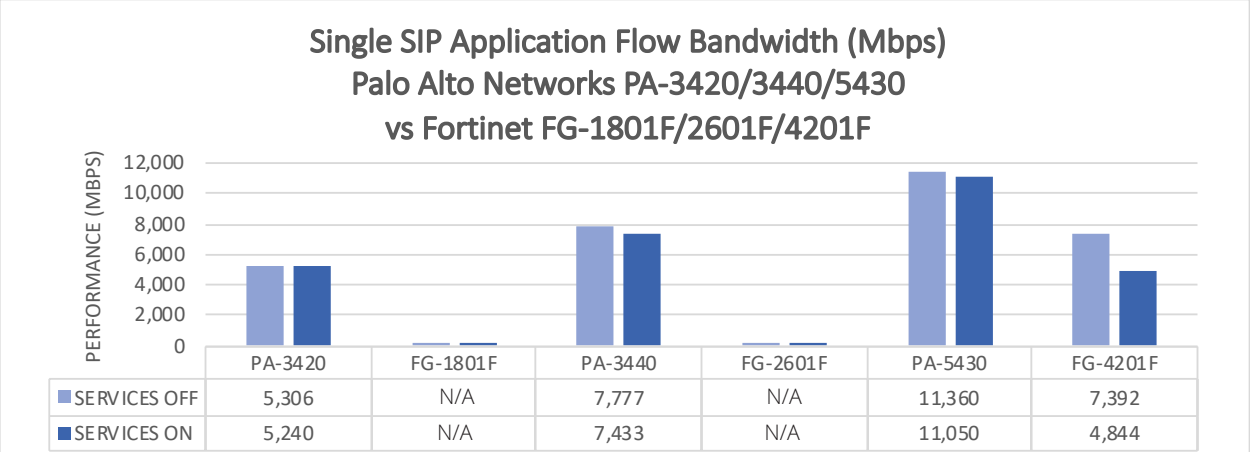
### 4.5K Payload

For bandwidth, Palo Alto Networks experienced a low average of 16 percent loss when services were enabled. Fortinet had significant loss in bandwidth - with an average of 48 percent degradation. For connection rate, Palo Alto Networks had an average of 42 percent decline in performance. Fortinet appliances, like bandwidth, saw a high loss of 76 percent on average.

## 5.3 Single Application Flow Bandwidth

Fortinet devices showed very low SIP throughput for FG-1801F and FG-2601F models. To work around the problem, the steps to disable SIP ALG listed in the knowledge base here (https://kb.fortinet.com/kb/documentLink.do?externalID=FD36405) were attempted, but it did not resolve the issue. It is our conclusion that SIP traffic is not being reliably processed by these FortiGate devices.

### 5.3.1 Session Initiation Protocol (SIP) Application Flow Bandwidth

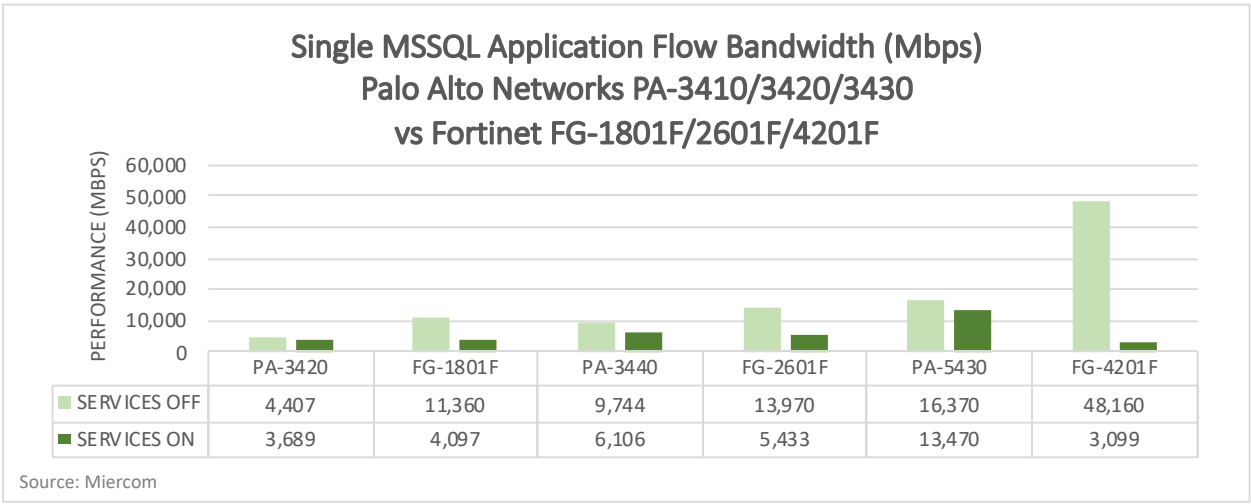



| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 5,306 | N/A | 7,777 | N/A | 11,360 | 7,392 |
| SERVICES ON | 5,240 | N/A | 7,433 | N/A | 11,050 | 4,844 |

Source: Miercom

*With services enabled, Palo Alto Networks PA-3420 saw barely any loss in bandwidth at just 1.2 percent. Fortinet FG-1801F had negligible throughput, so degradation was not recorded. While PA-3440 had just 4.4 percent degradation. Like FG-1801F, FG-2601F had negligible throughout and, therefore, no degradation to record. PA-5430 degraded by2.7 percent, compared to FG-4201F which degraded by 34 percent.*

### 5.3.2 MSSQL Application Flow Bandwidth

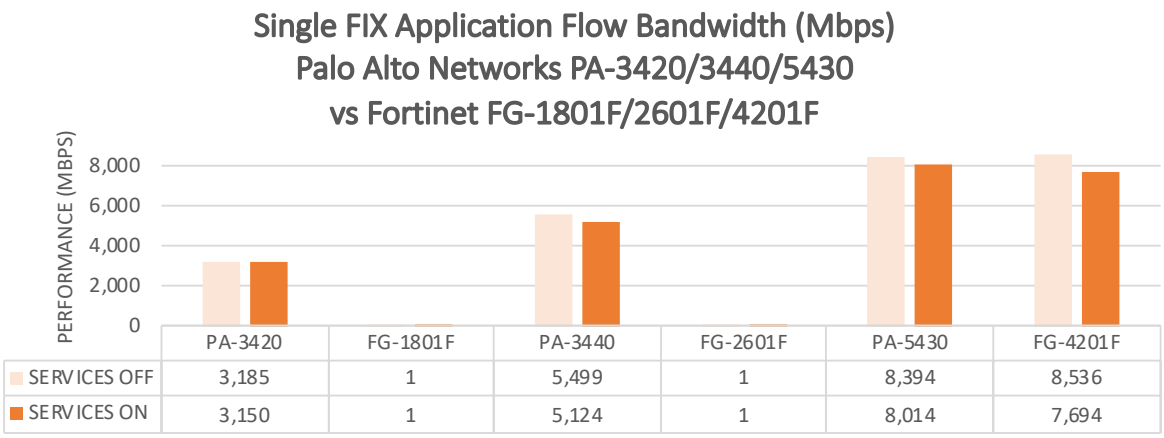



| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 4,407 | 11,360 | 9,744 | 13,970 | 16,370 | 48,160 |
| SERVICES ON | 3,689 | 4,097 | 6,106 | 5,433 | 13,470 | 3,099 |

Source: Miercom

*With services enabled, Palo Alto Networks PA-3420 saw 16 percent degradation, compared to Fortinet FG-1801F having a 64 percent loss. PA-3440 saw 37 percent degradation, whereas FG-2601F declined by 61 percent. PA-5430 saw 18 percent degradation, whereas FG-4201F saw a high loss of 94 percent.*

### 5.3.3 Financial Information eXchange (FIX) Application Flow Bandwidth

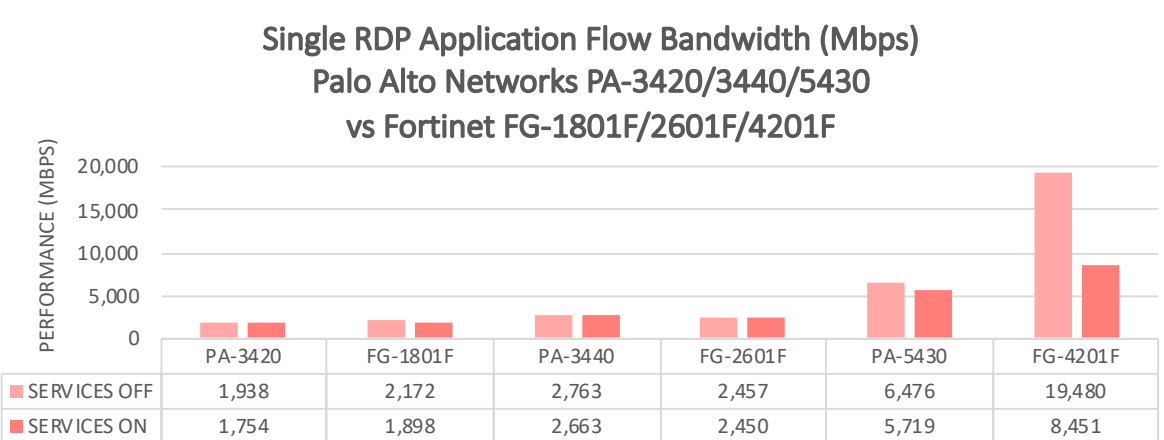



| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 3,185 | 1 | 5,499 | 1 | 8,394 | 8,536 |
| SERVICES ON | 3,150 | 1 | 5,124 | 1 | 8,014 | 7,694 |

Source: Miercom

*With services enabled, Palo Alto Networks PA-3420 saw negligible performance decline of just 1.1 percent. PA-3440 saw just 6.8 percent degradation with services turned on. The Fortinet FG-1801F and FG-2601F appliances were unable to process FIX application traffic. PA-5430 had 4.5 percent degradation, and FG-4201F had 10 percent loss of bandwidth.*

### 5.3.4 Remote Desktop Protocol (RDP) Application Flow Bandwidth




| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 1,938 | 2,172 | 2,763 | 2,457 | 6,476 | 19,480 |
| SERVICES ON | 1,754 | 1,898 | 2,663 | 2,450 | 5,719 | 8,451 |

Source: Miercom

*With services enabled, Palo Alto Networks PA-3420 saw 9.5 percent degradation, compared to Fortinet FG-1801F having a 13 percent loss. PA-3440 saw only 3.6 percent degradation; FG-2601F declined by 0.28 percent. PA-5430 saw 12 percent degradation, whereas FG-4201F saw 57 percent loss.*

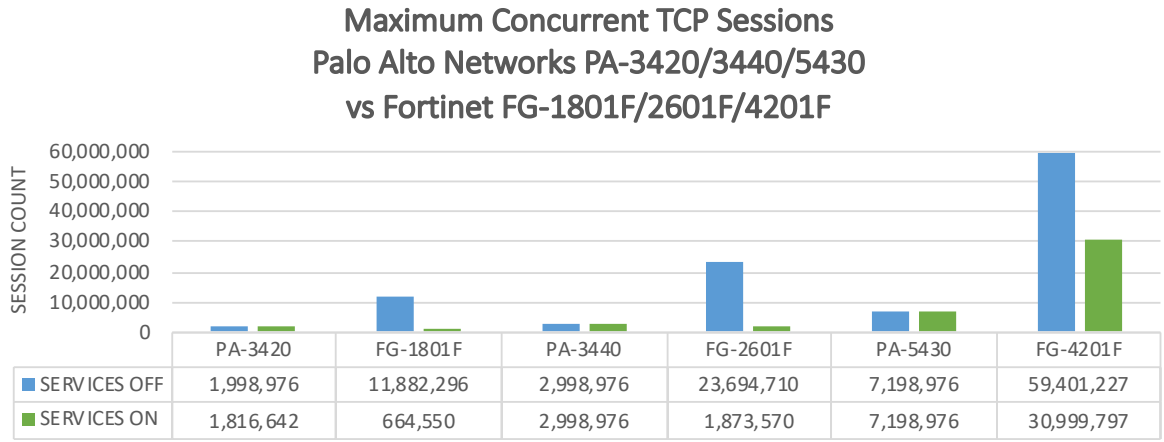
## The Palo Alto Networks Advantage

Fortinet FG-1801 and FG-2601F appliances were unable to process FIX traffic causing 100 percent traffic loss. These same models also achieved very low throughput for SIP protocol, making them not deployable where FIX or SIP protocols are required. The Palo Alto appliances, on the other hand, were able to reliably process all four real-world applications tested with consistent performance even with services disabled.

## 5.4 TCP Maximum Capacity

This section covers two tests: Maximum Concurrent TCP Sessions and Maximum TCP Connections per Second. This test used the BreakingPoint's Application Simulator component and a 1-byte HTTP 1.1 payload (no compression). We ran each test until the TCP reset rate equals 1% of the maximum attempted connections, and measured session count and connection rate with security enabled and disabled.

### 5.4.1 Maximum Concurrent TCP Sessions

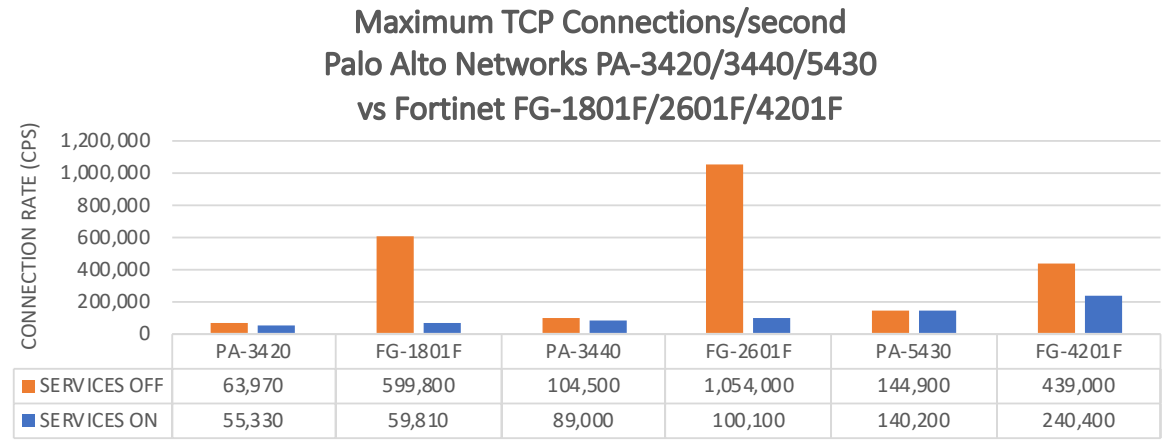



| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 1,998,976 | 11,882,296 | 2,998,976 | 23,694,710 | 7,198,976 | 59,401,227 |
| SERVICES ON | 1,816,642 | 664,550 | 2,998,976 | 1,873,570 | 7,198,976 | 30,999,797 |

Source: Miercom

*Once services were enabled, Palo Alto Networks PA-3420 session count degraded by just 9 percent, whereas Fortinet FG-1801F saw a steep decline of 95 percent. PA-3440 session count saw no change with services enabled, compared to FG-2601F showed significantly more loss of 92 percent. PA-5430 did not experience any performance loss; FG-4201F declined by almost 50 percent.*

### 5.4.2 Maximum TCP Connections/sec (CPS)




| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 63,970 | 599,800 | 104,500 | 1,054,000 | 144,900 | 439,000 |
| SERVICES ON | 55,330 | 59,810 | 89,000 | 100,100 | 140,200 | 240,400 |

Source: Miercom

*Once services were enabled, Palo Alto Networks PA-3420 connection rate declined by 14 percent; Fortinet FG-1801F showed significant degradation of 90 percent. PA-3440 fell by 15 percent, while FG-2601F dropped by 91 percent. PA-5430 experienced only a 3.2 percent decrease, but FG-4201F dropped by 45 percent.*

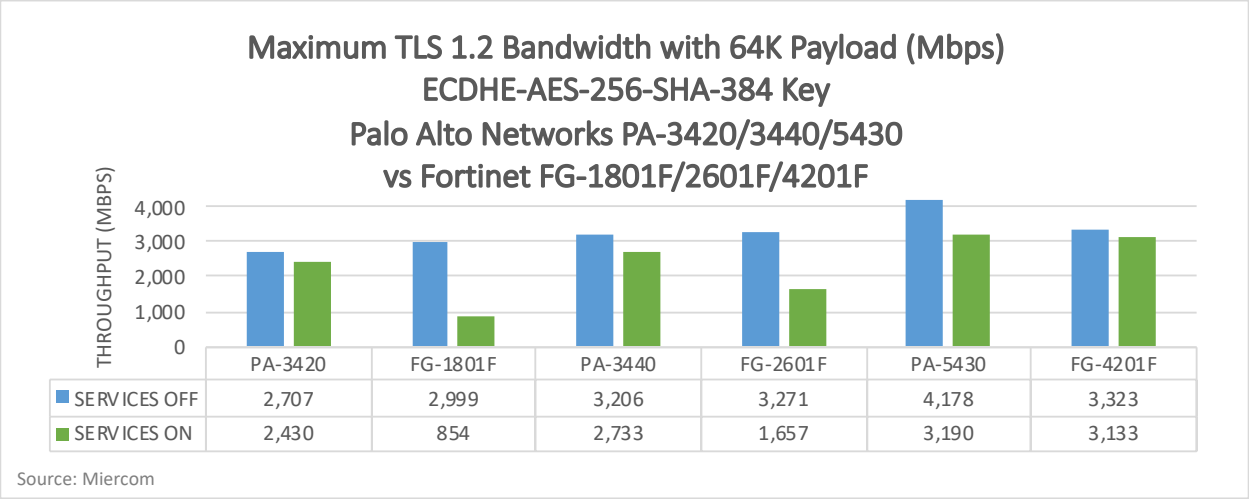
## The Palo Alto Networks Advantage

Palo Alto Networks appliances were observed having an average just 3 percent decline in TCP sessions once services were enabled. Fortinet had over 26 times the loss - at 78 percent average degradation. For connection rate, Palo Alto Networks experienced an average decline of just 11 percent, compared to Fortinet's significant 75 percent drop.

## 5.5 Maximum TLS 1.2 Bandwidth

This test evaluated encrypted performance using an HTTP Get/Response with a static payload of 64KB. The Keysight tool "IxLoad" simulated the most popular TLS 1.2 cipher suites: ECDHE- AES-256-SHA-384-64K-4K-key, ECDSA-AES-128-GCM-SHA256_P521-key, ECDHE-AES-128-SHA-256-2K-key. The ramp rate for these tests were configured to attempt to achieve 100Gb/sec. Similar to the unencrypted HTTP GET/Response cases, this test was considered in a failure state once TCP Concurrent sessions show an exponential increase and/or application transactions exceed 1% of the total attempted application transactions. Traffic throughput was recorded, with both security services enabled and disabled.

### 5.5.1 ECDHE-AES-256-SHA-384 Key

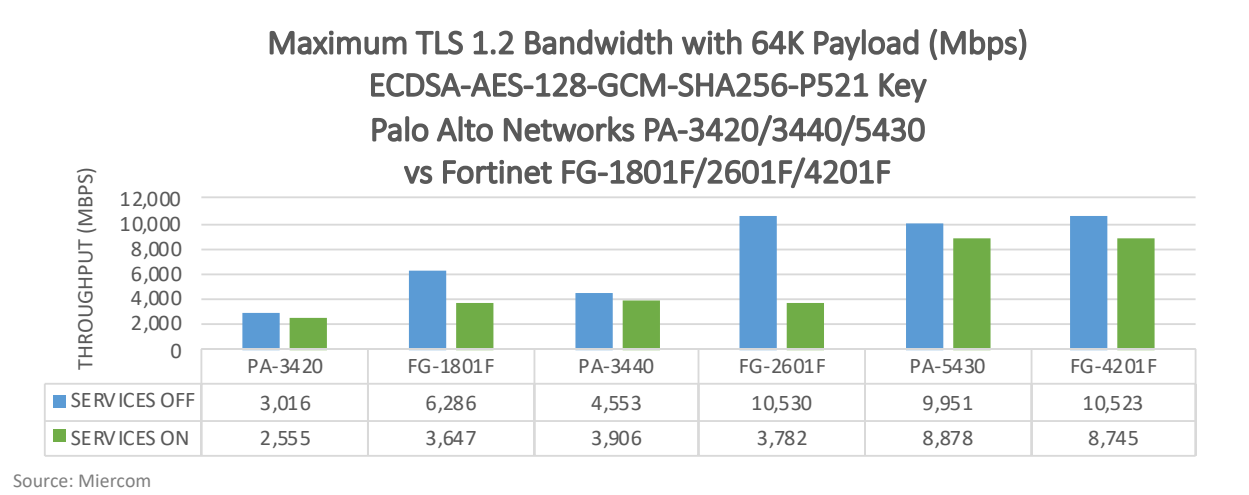



| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 2,707 | 2,999 | 3,206 | 3,271 | 4,178 | 3,323 |
| SERVICES ON | 2,430 | 854 | 2,733 | 1,657 | 3,190 | 3,133 |

Source: Miercom

*Once services were enabled, Palo Alto Networks PA-3420 throughput degraded by 10 percent, whereas Fortinet FG-1801F saw significant decline of 72 percent. PA-3440 saw 15 percent loss, compared to FG-2601F which fell by 49 percent. PA-5430 performance decreased by 24 percent; FG-4201F declined by just 6 percent.*

### 5.5.2 ECDSA-AES-128-GCM-SHA256-P521 Key

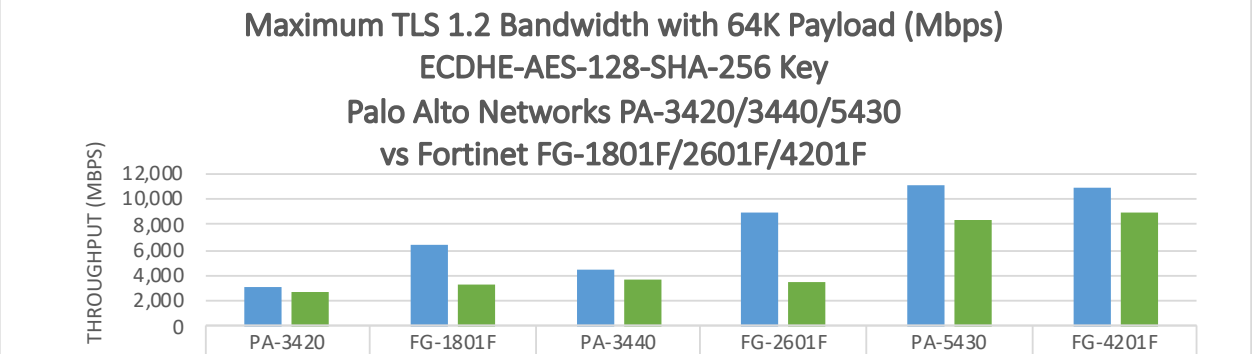



| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 3,016 | 6,286 | 4,553 | 10,530 | 9,951 | 10,523 |
| SERVICES ON | 2,555 | 3,647 | 3,906 | 3,782 | 8,878 | 8,745 |

Source: Miercom

*Once services were enabled, Palo Alto Networks PA-3420 throughput degraded by 15 percent, whereas Fortinet FG-1801F saw 42 percent loss. PA-3440 fell by 14 percent, compared to FG-2601F which had a significant loss of 64 percent. PA-5430 performance decreased by 11 percent; FG-4201F declined by 17 percent.*

### 5.5.3 ECDHE-AES-128-SHA-256 Key




| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 3,051 | 6,383 | 4,419 | 8,951 | 11,118 | 10,876 |
| SERVICES ON | 2,765 | 3,264 | 3,620 | 3,416 | 8,341 | 8,958 |

Source: Miercom

*Once services were enabled, Palo Alto Networks PA-3420 performance declined by 9.4 percent; Fortinet FG-1801F showed significant degradation of nearly 50 percent. PA-3440 fell by 18 percent, while FG-2601F saw a large drop of 62 percent. PA-5430 experienced only a 25 percent decrease; FG-4201F dropped by 18 percent.*

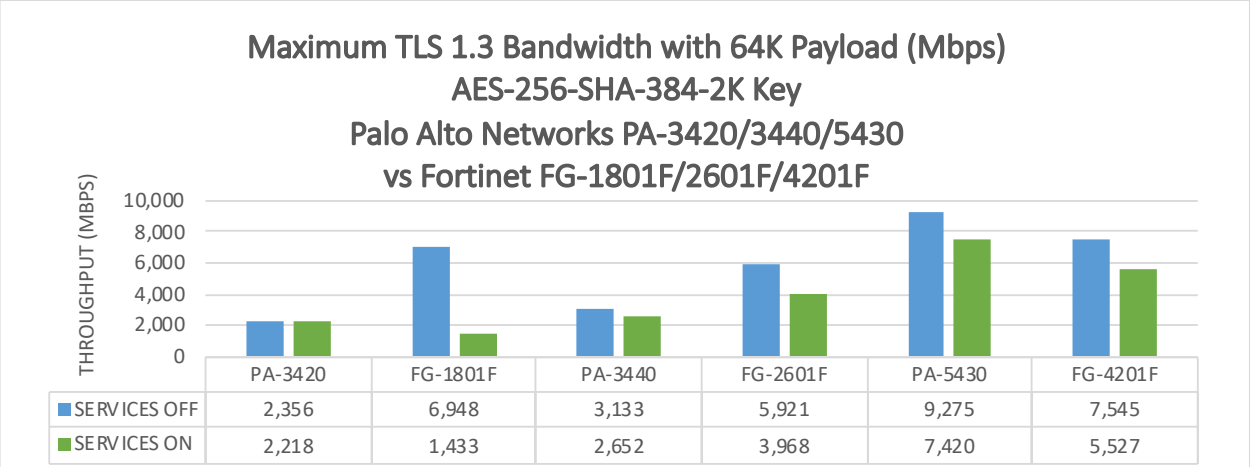
## The Palo Alto Networks Advantage

Palo Alto Networks appliances were observed having an average 18 percent decline in throughput once services were enabled. Fortinet had 2.4 times the loss - at 43 percent average degradation.

## 5.6 Maximum TLS 1.3 Bandwidth

This test assessed encrypted performance using an HTTP GET/Response with a static payload of 64KB. The Keysight tool "BreakingPoint" simulated the most popular TLS 1.3 cipher suite: ECDSA-AES 256 SHA 384 2K Key. The ramp rate for these tests were configured in IxLoad to attempt to achieve 100Gb/sec. Just as with the TLS 1.2 cases, this test was considered a failure state once TCP Concurrent sessions showed an exponential increase and/or application transactions exceed 1% of the total attempted application transactions. Traffic throughput was recorded, with both security services enabled and disabled.

### 5.6.1 ECDHE-AES-256-SHA-384-2K Key




| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 2,356 | 6,948 | 3,133 | 5,921 | 9,275 | 7,545 |
| SERVICES ON | 2,218 | 1,433 | 2,652 | 3,968 | 7,420 | 5,527 |

Source: Miercom

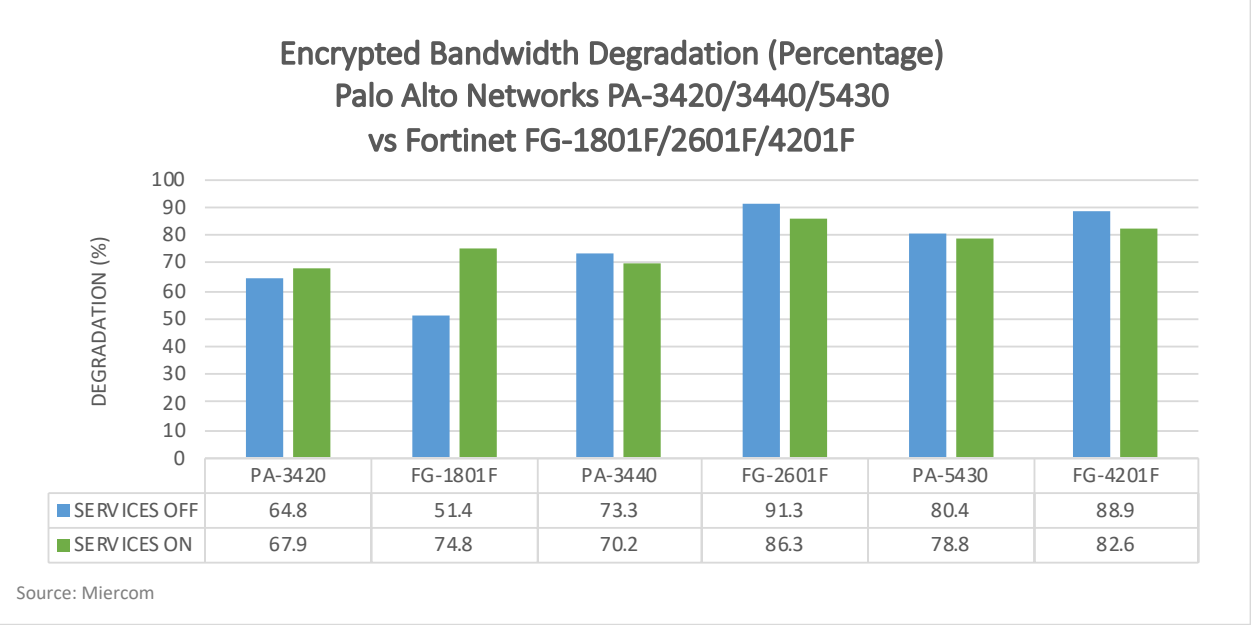
*Once services were enabled, Palo Alto Networks PA-3420 throughput degraded by just 5.9 percent, whereas Fortinet FG-1801F saw significant decline of 79 percent. PA-3440 saw 15 percent loss, compared to FG-2601F which fell by 33 percent. PA-5430 performance decreased by 20 percent; FG-4201F declined by 27 percent.*

## The Palo Alto Networks Advantage

Palo Alto Networks appliances were observed having an average 14 percent decline in throughput once services were enabled. Fortinet had 3.3 times the loss - at 46 percent average degradation.

## 5.7 Encrypted Bandwidth Degradation

This test compared encrypted and unencrypted bandwidth for a 64KB payload seen in Sections 5.2 and 5.6. The encryption standard used was TLS 1.3. This comparison was intended to show the degradation effect of encryption security seen by each product, with security features enabled and disabled.




| | PA-3420 | FG-1801F | PA-3440 | FG-2601F | PA-5430 | FG-4201F |
|---|---|---|---|---|---|---|
| SERVICES OFF | 64.8 | 51.4 | 73.3 | 91.3 | 80.4 | 88.9 |
| SERVICES ON | 67.9 | 74.8 | 70.2 | 86.3 | 78.8 | 82.6 |

Source: Miercom

*Once services were enabled, Palo Alto Networks PA-3420 saw up to 68 percent degradation in throughput when encryption standard TLS 1.3 was enabled for HTTP GET responses with a 64K payload. Fortinet FG-1801F saw up to 75 percent. PA-3440 saw up to 73 percent degradation, but FG-2601F saw as high as 91 percent. PA-5430 saw degradation of 80 percent, but FG-4201F saw as high as 89 percent loss.*

## The Palo Alto Networks Advantage

Palo Alto Networks appliances were observed having lower average degradation for encrypted traffic than Fortinet products, regardless of services on or off. For services disabled, Palo Alto Networks saw an average of 5 percent lower than its Fortinet counterparts - with a high of 25 percent less loss. For services enabled, Palo Alto Networks saw an average of 13 percent lower - with a high of 23 percent less loss.

# Total Cost of Ownership

6

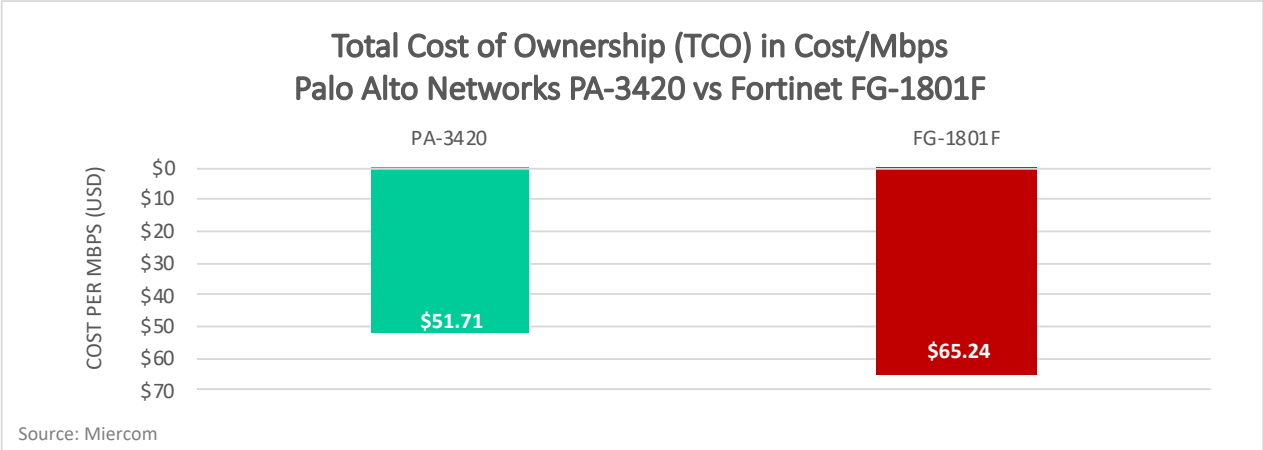
As with performance testing, we compared NGFW products for their performance and cost-benefit value in Cost per Mbps (USD). We evaluated the average throughput (in Mbps) and total cost of acquirement (hardware, subscription and support pricing). Average throughput was weighted using a mixture of 30 percent non-TLS throughput and 70 percent TLS throughput. The following tables and charts provide details on the total Cost/Mbps calculations for each comparable pair.

| Palo Alto Networks TCO Calculations | | | | | |
|---|---|---|---|---|---|
| Product | **Average Throughput (Mbps)** | **Total Cost (USD)** | **Hardware Cost (USD)** | **Subscription & Support Cost (USD)** | **Cost/Mbps** |
| PA-3420 | 2,911.10 | ***$150,545.00*** | $41,700.00 | $108,845.00 | ***$51.71*** |
| PA-3440 | 4,128.61 | ***$222,380.00*** | $61,600.00 | $160,780.00 | ***$53.86*** |
| PA-5430 | 9,179.84 | ***$613,245.00*** | $210,000.00 | $403,245.00 | ***$66.80*** |

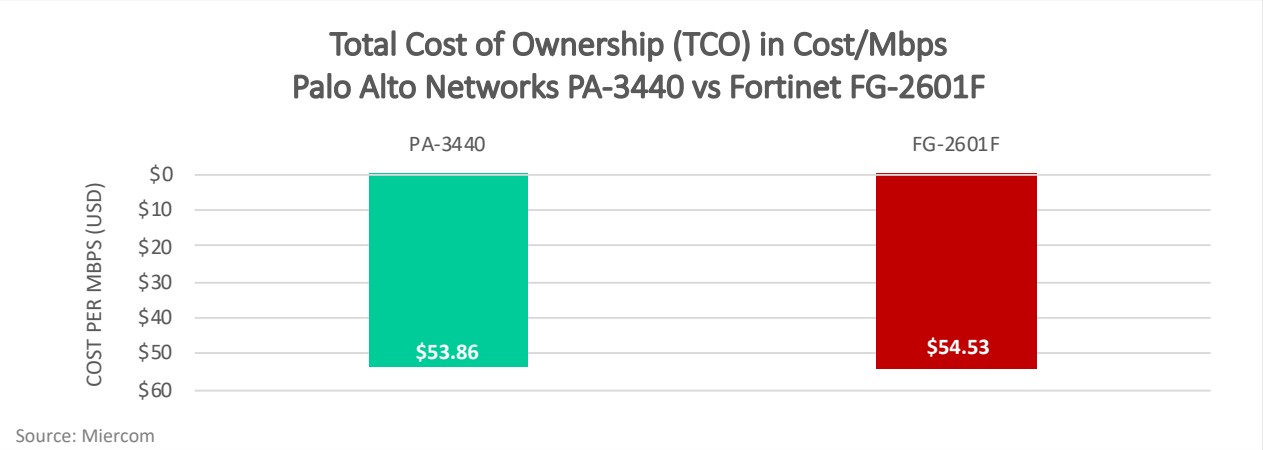
| Fortinet FortiGate TCO Calculations | | | | | |
|---|---|---|---|---|---|
| Product | **Average Throughput (Mbps)** | **Total Cost (USD)** | **Hardware Cost (USD)** | **Subscription & Support Cost (USD)** | **Cost/Mbps** |
| FG-1801F | 2,262.36 | ***$147,603.25*** | $50,035.00 | $97,568.00 | ***$65.24*** |
| FG-2601F | 3,955.83 | ***$215,727.60*** | $73,128.00 | $142,600.00 | ***$54.53*** |
| FG-4201F | 9,146.08 | ***$663,044.00*** | $224,761.00 | $438,283.00 | ***$72.49*** |

| Comparative Price and TCO Calculations: Palo Alto Networks vs Fortinet | | |
|---|---|---|
| Product Comparison | **Price Difference (Hardware and Subscriptions)** | **TCO per Protected Mbps Difference** |
| PA-3420 vs FG-1801F | ***2.0%*** | ***-26.2%*** |
| PA-3440 vs FG-2601F | ***3.0%*** | ***-1.2%*** |
| PA-5430 vs FG-4201F | ***-8.1%*** | ***-8.5%*** |

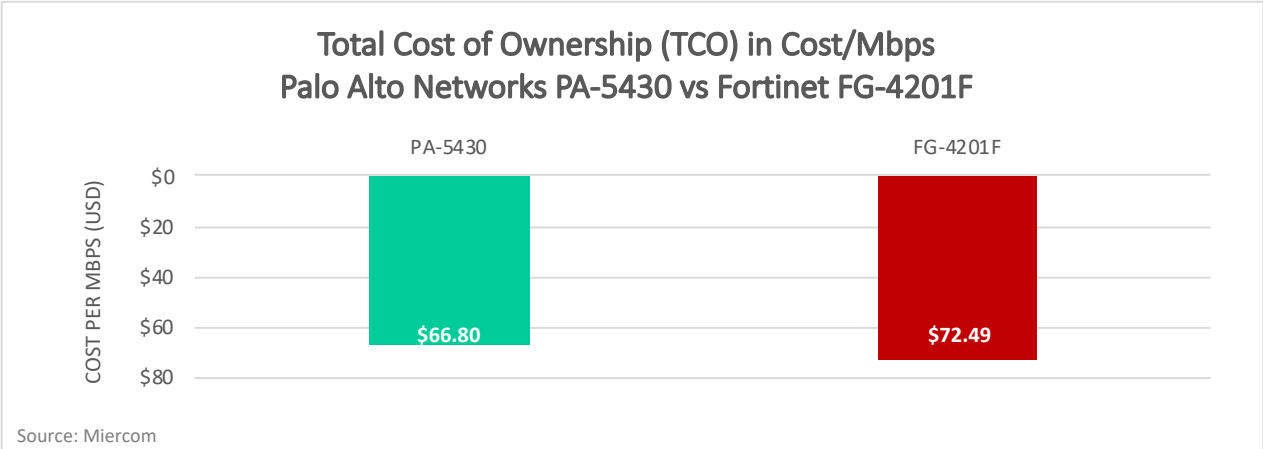
*Note: The the total costs of acquisition are based on prices as of May 1, 2022.*




*Palo Alto Networks PA-3420 offers a 26 percent cost savings per Mbps when compared to the Fortinet FG-1801F appliance, which has a higher cost of about $65 per Mbps. Fortinet costs more in hardware, subscriptions and support, while providing slightly lower average performance. PA-3420 had an average throughput of 2,911 Mbps, compared to the 2,262 Mbps seen by FG-1801F.*




*Palo Alto Networks PA-3440 offers 1.2 percent cost savings per Mbps when compared to the Fortinet FG-2601F appliance, Fortinet costs slightly more in hardware, subscriptions and support, while providing less performance. PA-3440 had an average throughput of 4,129 Mbps, compared to the 3,956 Mbps seen by FG-2601F.*




*Palo Alto Networks PA-5430 offers 8.5 percent cost savings per Mbps when compared to the Fortinet FG-4201F appliance, Fortinet costs more in hardware, subscriptions and support, while providing less performance. PA-5430 had an average throughput of 9,180 Mbps, compared to the 9,146 Mbps seen by FG-4201F.*

# 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 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
- **Advanced 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

*Fortinet devices showed very low SIP throughput. To work around the problem, the steps to disable SIP ALG listed in the knowledge base here (https://kb.fortinet.com/kb/documentLink.do?externalID=FD36405) were attempted, but it did not resolve the issue. It is our conclusion that SIP traffic is not being reliably processed by these FortiGate devices.*

| Test | PA-3420 | | | FG-1801F | | |
|---|---|---|---|---|---|---|
| | Services off | Services on | Degradation (%) | Services off | Services on | Degradation (%) |
| **5.1 Raw TCP Throughput with 1460-Byte Payload (Mbps)** | | | | | | |
| | 4965 | 4315 | 13.09% | 7154 | 3354 | 53.12% |
| **5.2 Maximum HTTP 1.1 Connections/sec (CPS) and Bandwidth (Mbps) with 64/21/4.5K Payload** | | | | | | |
| **64K Bandwidth** | 7912 | 7764 | 1.9% | 11640 | 9137 | 21.5% |
| **64K CPS** | 13090 | 12880 | 1.6% | 24990 | 20030 | 19.8% |
| **21K Bandwidth** | 3150 | 3049 | 3.21% | 4100 | 3334 | 18.7% |
| **21K CPS** | 16700 | 11450 | 31.44% | 134700 | 35240 | 73.8% |
| **4.5K Bandwidth** | 2322 | 2151 | 7.4% | 40140 | 37820 | 5.8% |
| **4.5K CPS** | 24410 | 2545 | 89.6% | 451100 | 47390 | 89.5% |
| **5.3 Single Application Performance (Mbps) before "Application Transaction Failures" exceed 20** | | | | | | |
| **SIP (Telephony)** | 5306 | 5240 | 1.24% | N/A | N/A | N/A |
| **MSSQL (Database)** | 4407 | 3689 | 16.3% | 11360 | 4097 | 63.9% |
| **FIX (Financial)** | 3185 | 3150 | 1.1% | N/A | N/A | N/A |
| **RDP (Remote Desktop Protocol)** | 1938 | 1754 | 9.49% | 2172 | 1898 | 12.6% |
| **5.4 Maximum TCP Capacity Concurrent TCP Sessions and Connections/sec (CPS)** | | | | | | |
| **Max Concurrent TCP Sessions** | 1998976 | 1816642 | 9.12% | 11882296 | 664550 | 94.4% |
| **Max TCP CPS** | 63970 | 55330 | 13.5% | 599800 | 59810 | 90.0% |
| **5.5 Maximum TLS 1.2 Capacity** | | | | | | |
| **ECDHE-AES-256-SHA-384** | 2707 | 2430 | 10.2% | 2999 | 854 | 71.5% |
| **ECDSA-AES-128-GCM-SHA-256-P521** | 3016 | 2555 | 15.3% | 6286 | 3647 | 42.0% |
| **ECDHE-AES-128-SHA-256** | 3051 | 2765 | 9.4% | 6383 | 3264 | 48.9% |
| **5.6 Maximum TLS 1.3 Capacity** | | | | | | |
| **AES-256-SHA-384 4K Key** | 2356 | 2218 | 5.9% | 6948 | 1433 | 79.4% |

| Test | PA-3440 | | | FG-2601F | | |
|---|---|---|---|---|---|---|
| | Services off | Services on | Degradation (%) | Services off | Services on | Degradation (%) |
| **5.1 Raw TCP Throughput with 1460-Byte Payload (Mbps)** | | | | | | |
| | 6879 | 6859 | 0.29% | 41950 | 5545 | 86.78% |
| **5.2 Maximum HTTP 1.1 Connections/sec (CPS) and Bandwidth (Mbps) with 64/21/4.5K Payload** | | | | | | |
| **64K Bandwidth** | 14330 | 10820 | 24.50% | 82230 | 23330 | 71.60% |
| **64K CPS** | 37540 | 28740 | 23.40% | 136300 | 38790 | 71.50% |
| **21K Bandwidth** | 10620 | 7797 | 26.60% | 17430 | 4572 | 73.80% |
| **21K CPS** | 51260 | 37600 | 26.65% | 178900 | 51430 | 71.30% |
| **4.5K Bandwidth** | 3683 | 3043 | 17.38% | 28540 | 4316 | 84.90% |
| **4.5K CPS** | 67450 | 55900 | 17.10% | 530000 | 79820 | 84.90% |
| **5.3 Single Application Performance (Mbps) before "Application Transaction Failures" exceed 20** | | | | | | |
| **SIP (Telephony)** | 7777 | 7433 | 4.42% | N/A | N/A | N/A |
| **MSSQL (Database)** | 9744 | 6106 | 37.3% | 13970 | 5433 | 61.1% |
| **FIX (Financial)** | 5499 | 5124 | 6.8% | N/A | N/A | N/A |
| **RDP (Remote Desktop Protocol)** | 2763 | 2663 | 3.62% | 2457 | 2450 | 0.28% |
| **5.4 Maximum TCP Capacity Concurrent TCP Sessions and Connections/sec (CPS)** | | | | | | |
| **Max Concurrent TCP Sessions** | 2998976 | 2998976 | 0.00% | 23694710 | 1873570 | 92.09% |
| **Max TCP CPS** | 104500 | 89000 | 14.83% | 1054000 | 100100 | 90.5% |
| **5.5 Maximum TLS 1.2 Capacity** | | | | | | |
| **ECDHE-AES-256-SHA-384** | 3206 | 2733 | 14.8% | 3271 | 1657 | 49.3% |
| **ECDSA-AES-128-GCM-SHA-256-P521** | 4553 | 3906 | 14.2% | 10530 | 3782 | 64.1% |
| **ECDHE-AES-128-SHA-256** | 4419 | 3620 | 18.1% | 8951 | 3416 | 61.8% |
| **5.6 Maximum TLS 1.3 Capacity** | | | | | | |
| **AES-256-SHA-384 4K Key** | 3133 | 2652 | 15.4% | 5921 | 3968 | 33.0% |

| Test | PA-5430 | | | FG-4201F | | |
|---|---|---|---|---|---|---|
| | Services off | Services on | Degradation (%) | Services off | Services on | Degradation (%) |
| **5.1 Raw TCP Throughput with 1460-Byte Payload (Mbps)** | | | | | | |
| | 18660 | 17280 | 7.40% | 45760 | 17240 | 62.30% |
| **5.2 Maximum HTTP 1.1 Connections/sec (CPS) and Bandwidth (Mbps) with 64/21/4.5K Payload** | | | | | | |
| **64K Bandwidth** | 43990 | 32800 | 25.40% | 61600 | 41410 | 32.78% |
| **64K CPS** | 74480 | 54850 | 26.40% | 140300 | 93820 | 33.13% |
| **21K Bandwidth** | 25740 | 20740 | 19.40% | 46730 | 31190 | 33.30% |
| **21K CPS** | 124200 | 100100 | 19.40% | 220000 | 150500 | 31.60% |
| **4.5K Bandwidth** | 7553 | 5854 | 22.50% | 22010 | 10560 | 52.00% |
| **4.5K CPS** | 131200 | 104900 | 20.00% | 398100 | 190600 | 52.10% |
| **5.3 Single Application Performance (Mbps) before "Application Transaction Failures" exceed 20** | | | | | | |
| **SIP (Telephony)** | 11360 | 11050 | 2.73% | 7392 | 4844 | 34% |
| **MSSQL (Database)** | 16370 | 13470 | 17.7% | 48160 | 3099 | 93.6% |
| **FIX (Financial)** | 8394 | 8014 | 4.5% | 8536 | 7694 | 9.9% |
| **RDP (Remote Desktop Protocol)** | 6476 | 5719 | 11.69% | 19480 | 8451 | 56.62% |
| **5.4 Maximum TCP Capacity Concurrent TCP Sessions and Connections/sec (CPS)** | | | | | | |
| **Max Concurrent TCP Sessions** | 7198976 | 7198976 | 0.0% | 59,401,227 | 30,999,797 | 47.8% |
| **Max TCP CPS** | 144900 | 140200 | 3.2% | 439000 | 240400 | 45.2% |
| **5.5 Maximum TLS 1.2 Capacity** | | | | | | |
| **ECDHE-AES-256-SHA-384** | 4178 | 3190 | 23.6% | 3323 | 3133 | 5.7% |
| **ECDSA-AES-128-GCM-SHA-256-P521** | 9951 | 8878 | 10.8% | 10523 | 8745 | 16.9% |
| **ECDHE-AES-128-SHA-256** | 11118 | 8341 | 25.0% | 10876 | 8958 | 17.6% |
| **5.6 Maximum TLS 1.3 Capacity** | | | | | | |
| **AES-256-SHA-384 4K Key** | 9275 | 7420 | 20.0% | 7545 | 5527 | 26.7% |