Palo Alto Networks
Next-Generation Firewall (NGFW)
AI-Powered Prevention Performance

Detailed Report DR251029D

AI & Encrypted Traffic Performance Validation

TABLE OF CONTENTS

DR251029C

1 Executive Summary

DR251029C

Business networks are now dominated by highly dynamic AI and API traffic, creating new security and performance challenges that demand an AI-powered Next-Generation Firewall. As agent-based features spread, machine-to-machine calls and tool use across APIs are rising sharply, which means performance baselines, bursts and chained requests. At the same time, AI is being used in daily workflows. More than 70% of enterprise traffic is encrypted with TLS 1.2 and TLS 1.3, so platforms must inspect and process encrypted flows without affecting user experience.

By engaging Miercom to perform independent validation testing, Palo Alto Networks wants to show how enabling security services on the firewall improves ability to handle AI Traffic without degrading the performance. The PA-500 Series represents the next-generation security standard. The PA-560 and PA-520 are purpose-built and performance-optimized for the most demanding modern AI workloads—including large language model (LLM) traffic, high-volume streaming APIs, and intelligent agents. They focus on high throughput, high stability decryption, and strong concurrent session handling, with complete security enabled by default. This testing provides an independent, objective report that gives customers clear, credible insights into performance under real-world network conditions.

Tests emphasize security by default, with core services enabled and aligned for feature parity across vendors: including TLS and SSL decryption and inspection, and policy inspection in flow versus proxy mode. For Palo Alto Networks, services turned on included Threat Prevention (antivirus, vulnerability protection, anti-spyware, data filtering, basic file blocking), WildFire, decryption, and default application identification policies. For Fortinet devices, services on include Antivirus, IPS, File Filter, Email Filter, and decryption with equivalent default policies. Where useful, baseline measurements without inspection are used for reference. Agent activity introduces risks like prompt injection and unwanted tool access, so performance testing must include strong security controls, full encryption, strict access limits and validation that throughput remains steady under inspection.

Key Findings

- **Decisive AI Security Performance Advantage:** The PA-560 established clear, consistent leadership across all demanding AI-driven replay workloads (Perplexity, Grok, DeepSeek, OpenAI Playground), delivering 2× to over 8× the throughput of the FG-201G. Critically, the PA-520 outperformed the FG-71G in every single AI scenario tested, demonstrating Palo Alto Networks' superior AI readiness at every tier.
- **Leadership in Encrypted AI Traffic Processing:** With over 70% of enterprise traffic encrypted, Palo Alto Networks platforms sustained substantially and consistently higher throughput in both TLS 1.2 and TLS 1.3 decryption scenarios than equivalent Fortinet models, proving superior protection and performance for modern, encrypted AI and API traffic Superior Stability and Unmatched Performance under Load. In stark contrast to the PA-560 and PA-520, which maintained uninterrupted operational stability under all test conditions, the Fortinet FG-201G failed a critical AI-traffic test (DeepSeekAI) by repeatedly entering memory-induced Conserve Mode and also during Maximum Connections per second and Maximum Concurrent connections test. This fundamental design limitation caused memory exhaustion *before* CPU utilization was maxed out, demonstrating the platform's critical inability to sustain modern, security-intensive AI workloads. The PA-560,

by contrast, maintained superior stability and memory resource management under identical load.

- **Superior Application Traffic Scalability:** Proving Enterprise Readiness. The expanded application suite (SIP, MSSQL, FIX, RDP, SMBv2, FTP) is essential because it simulates a realistic, complex enterprise network environment that relies on specialized, high-demand protocols beyond standard web traffic. By handling this diverse, challenging mix, Palo Alto Networks platforms maintained throughput across all tested flows. In stark contrast, Fortinet devices exhibited severe throughput drops or failed completely to process certain critical protocols (like FIX), proving their inability to scale reliably in a true enterprise setting. Significant Total Cost-of-Ownership Advantage. Across both the PA-560 and PA-520 comparisons, Palo Alto Networks delivered a lower cost per Mbps than Fortinet alternatives. The cost advantage ranged from 30% to over 60%, driven by higher protected throughput and more efficient hardware utilization.

It is important to consider proper product sizing when deploying an NGFW appliance. Metrics for each product are observed in the intended network environment to yield optimal, but realistic, performance with security enabled by default. Datasheet claims often do not reflect real deployments, especially with services turned on, which can give a false impression of protection and performance. We used each product as any customer would in terms of real world scenarios, providing objective and practical results.

Based on our observations, we found the Palo Alto Networks Next Generation Firewall PA-560/520 appliances to have superior performance in multiple real-world network scenarios, with and without security features enabled. Ultimately, the PA-500 Series offered superior, AI-ready performance at a lower TCO, establishing Palo Alto Networks as the clear, future-proof choice for organizations prioritizing security and scalability against emerging AI-driven threats. We proudly award Palo Alto Networks the ***Miercom Performance Verified*** certification in recognition of its impressive competitive performance.

Rob Smithers

CEO, Miercom

2 Test Summary

DR251029C

The comparative analysis below highlights the performance and total cost of ownership (TCO) observed across tested next-generation firewall platforms. Each device was evaluated under identical real-world traffic conditions with security services enabled, ensuring consistency in performance measurement. The results demonstrated how throughput and TCO per protected Mbps scale across product families, providing clear visibility into performance-per-dollar and overall platform value. The chart summarizes these findings illustrating how each solution performs compared to Fortinet model.

	PA-560	FG-201G	PA-520	FG-71G
Average Throughput with Services Enabled (Mbps)	**3375**	**1813**	**685**	**273**
TCO per Protected Mbps (Pro-Bundle for Palo Alto Networks, UTP Bundle for Fortinet)	**$9.21**	**$14.90**	**$7.30**	**$12.38**
Throughput Comparison	**PA-560 throughput is 1.9x better than FG-201G** **The PA-560's throughput is 86.2% higher than the FG-201G.**		**PA-520 throughput is 2.5x better than FG-71G** **The PA-520's throughput is 150% higher than the FG-71G.**	
TCO Comparison	**PA-560 TCO is 1.6x better than FG-201G**		**PA-520 TCO is 1.7x better than FG-71G**	
Cost Efficiency in %	**PA-560 is 32% more cost-efficient per stable Mbps**		**PA-520 is 70% more cost-efficient per stable Mbps**	

Palo Alto Networks PA-550/520 Next Generation Firewall

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

PA-560

Version 12.1.2

PA-520

Version 12.1.2

Services on:

- Advanced Threat Prevention
- Anti-Virus Protection
- Anti-Spyware Protection
- Application ID/Control
- File Blocking - Basic
- WildFire protection
- SSL Inspection (profiles to be adjusted per test)

Fortinet FortiGate 201G/71G Network Firewall

FG-201G

Version: 7.2.11 build6561

FG-71G

Version: 7.2.11 build6561

Services on:

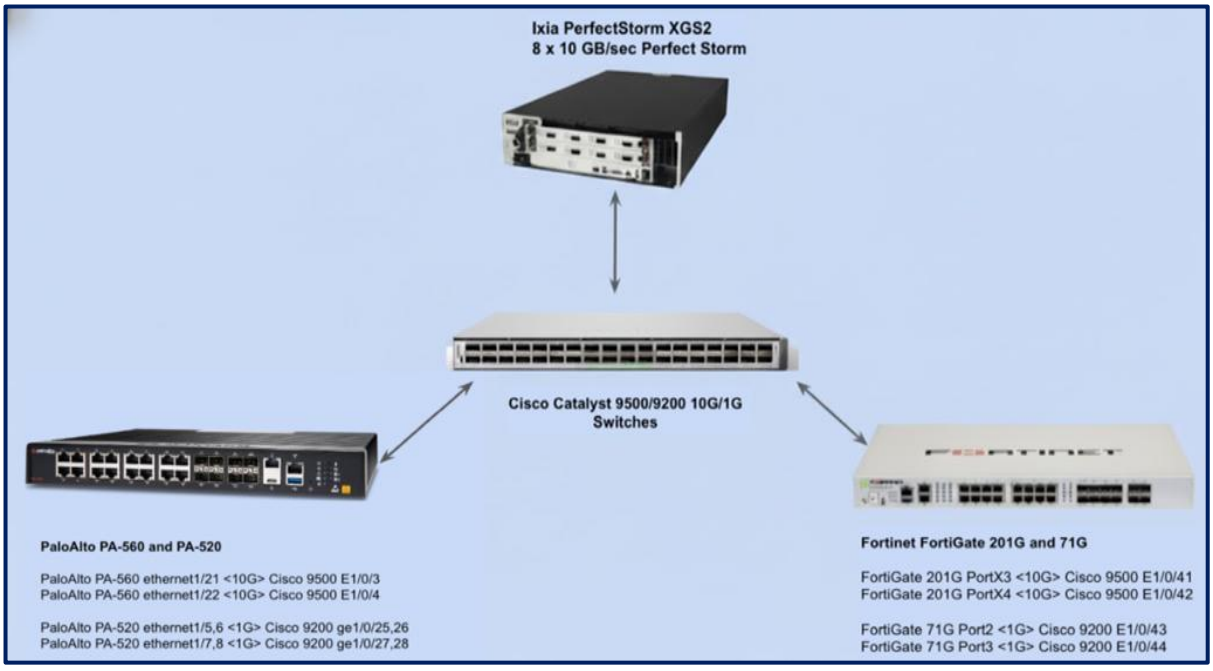
- Anti-Virus Protection
- Application Control
- IPS
- File Filter
- SSL Inspection (profiles to be adjusted per test)

Using hands-on network testing tools, we simulated business environments and exercised each device with real traffic to provide an accurate assessment of product performance. The traffic mix reflected today's usage, including encrypted applications, API-heavy flows, and multi-step AI workflows that create short bursts, chained requests, and higher concurrency.

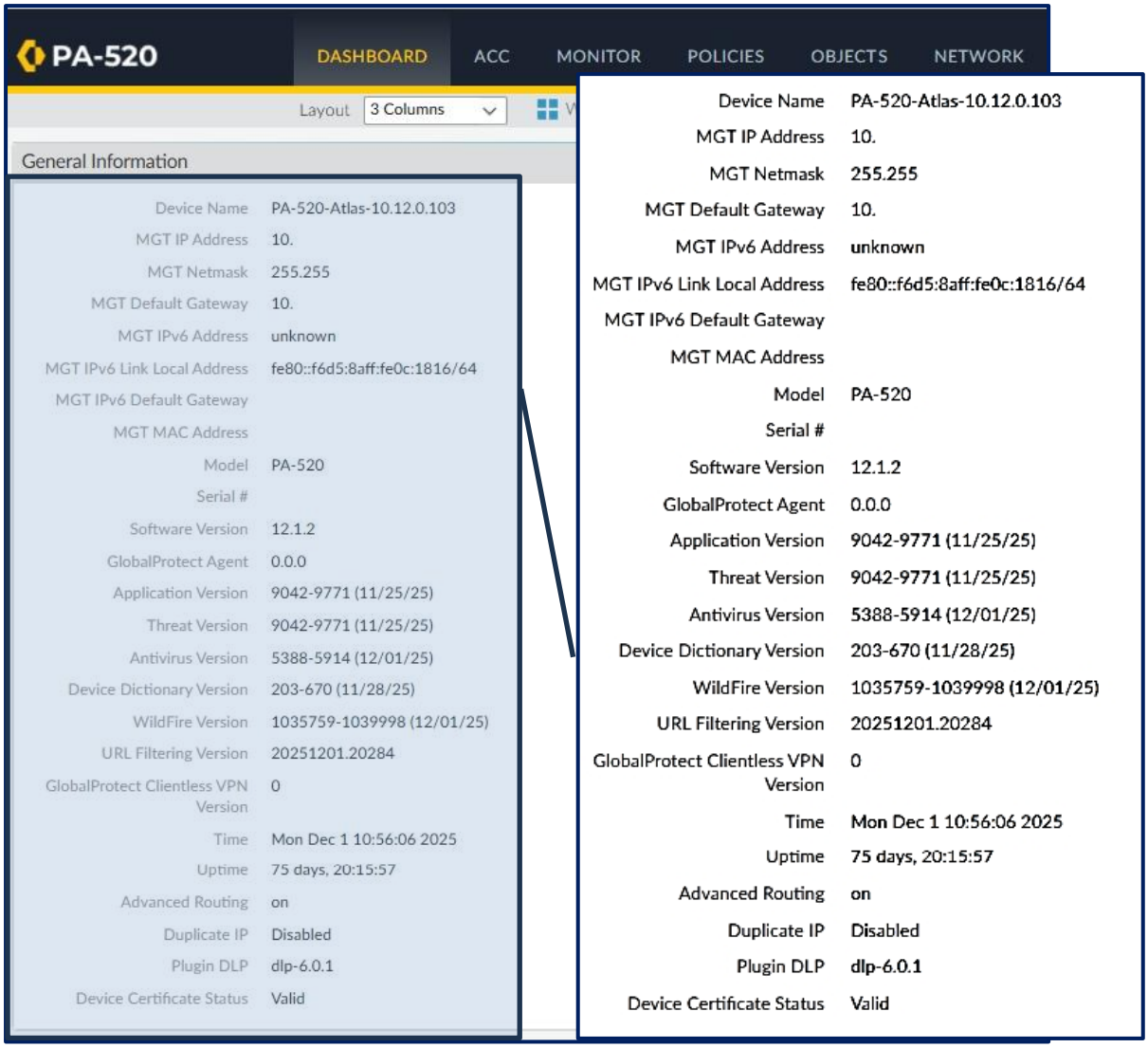
The Palo Alto Networks and Fortinet appliances were compared using application traffic generated by Ixia BreakingPoint PerfectStorm with an 8×10 Gb per second card, GA software, and current ATI, while services were disabled and enabled on the device. Platforms under test were Palo Alto Networks PA-500 Series models PA-560, PA-520, and Fortinet FortiGate G-Series models 201G and 71G. Scope included Security by Default policy inspection in Flow and Proxy mode, along with TLS and SSL decryption and inspection. Primary KPI was Ethernet Data Rate in Gbps under real workload conditions. Tests ran until a defined threshold was reached, such as more than 100 application transaction failures or 90% CPU utilization, at which point the observed bandwidth was recorded as the maximum for that workload.

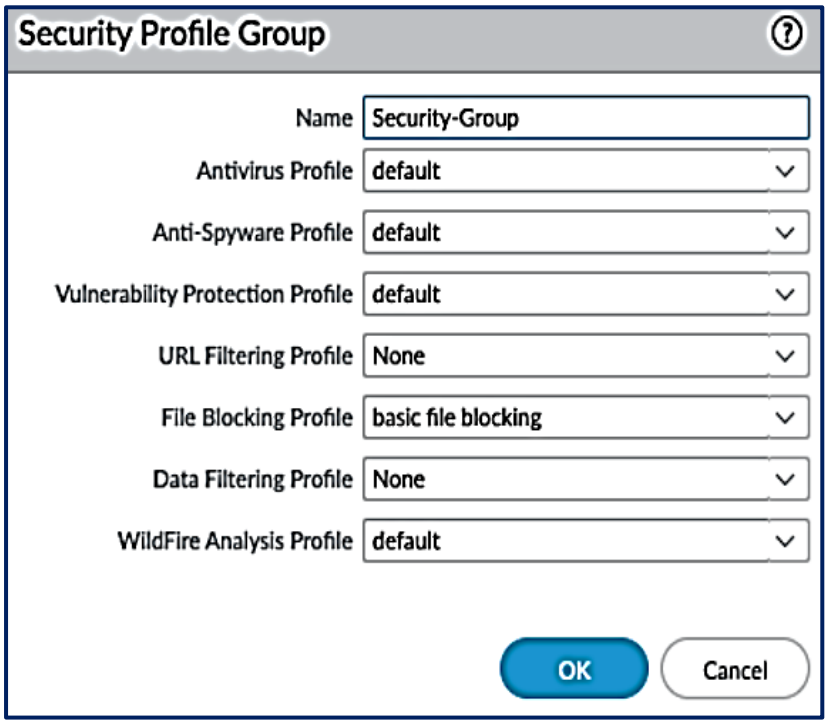
All devices were configured to have security disabled /services off and then security enabled /services on. For Palo Alto Networks, services turned on included Threat Prevention (antivirus, vulnerability protection, anti-spyware, data filtering, basic file blocking), WildFire, decryption, and default application identification policies. For Fortinet devices, services on included Antivirus, IPS, Default File Filter, decryption, and equivalent default policies, with policy levels aligned for feature parity across platforms. AI workflow traffic was drawn from four representative classes: text generation APIs, multimodal image and video tasks, IDE-integrated coding assistants, and search and knowledge platforms. All workloads used real TLS sessions or ATI super flows to ensure realism.

Test Topology

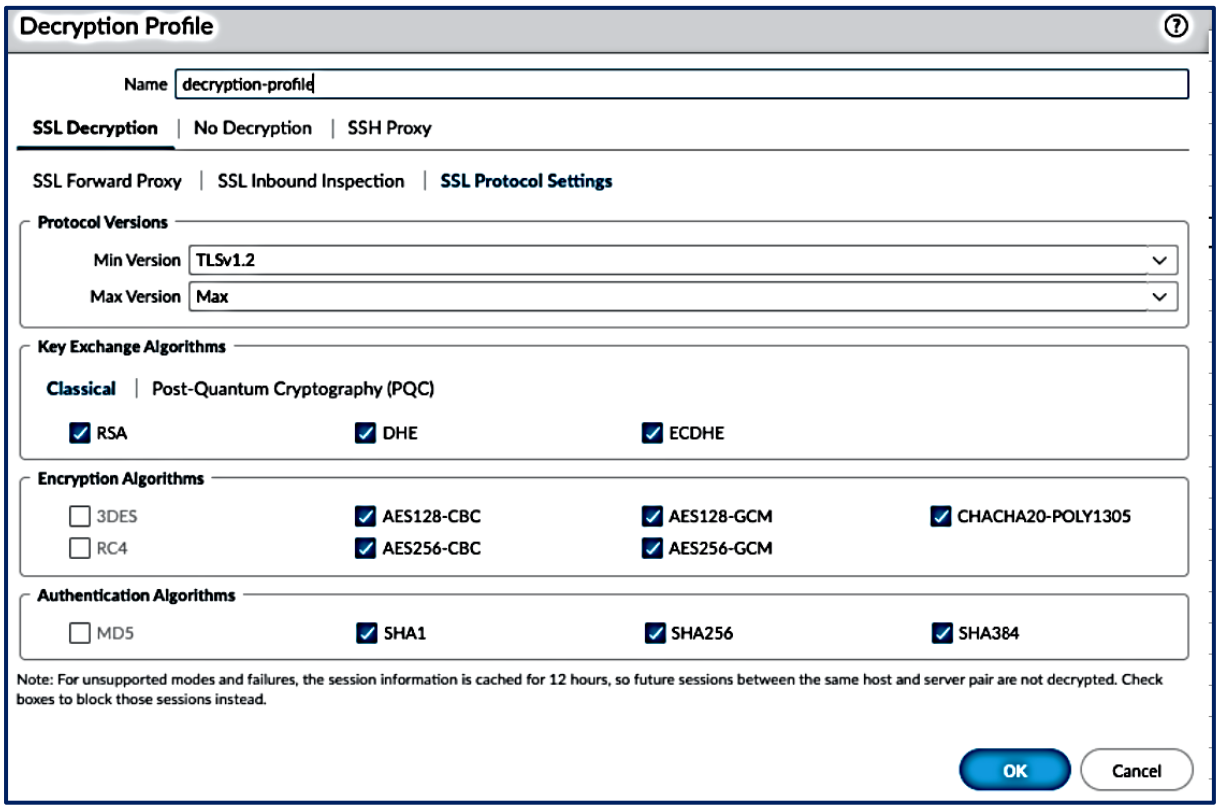


Palo Alto Networks 500 series Firewall Configuration

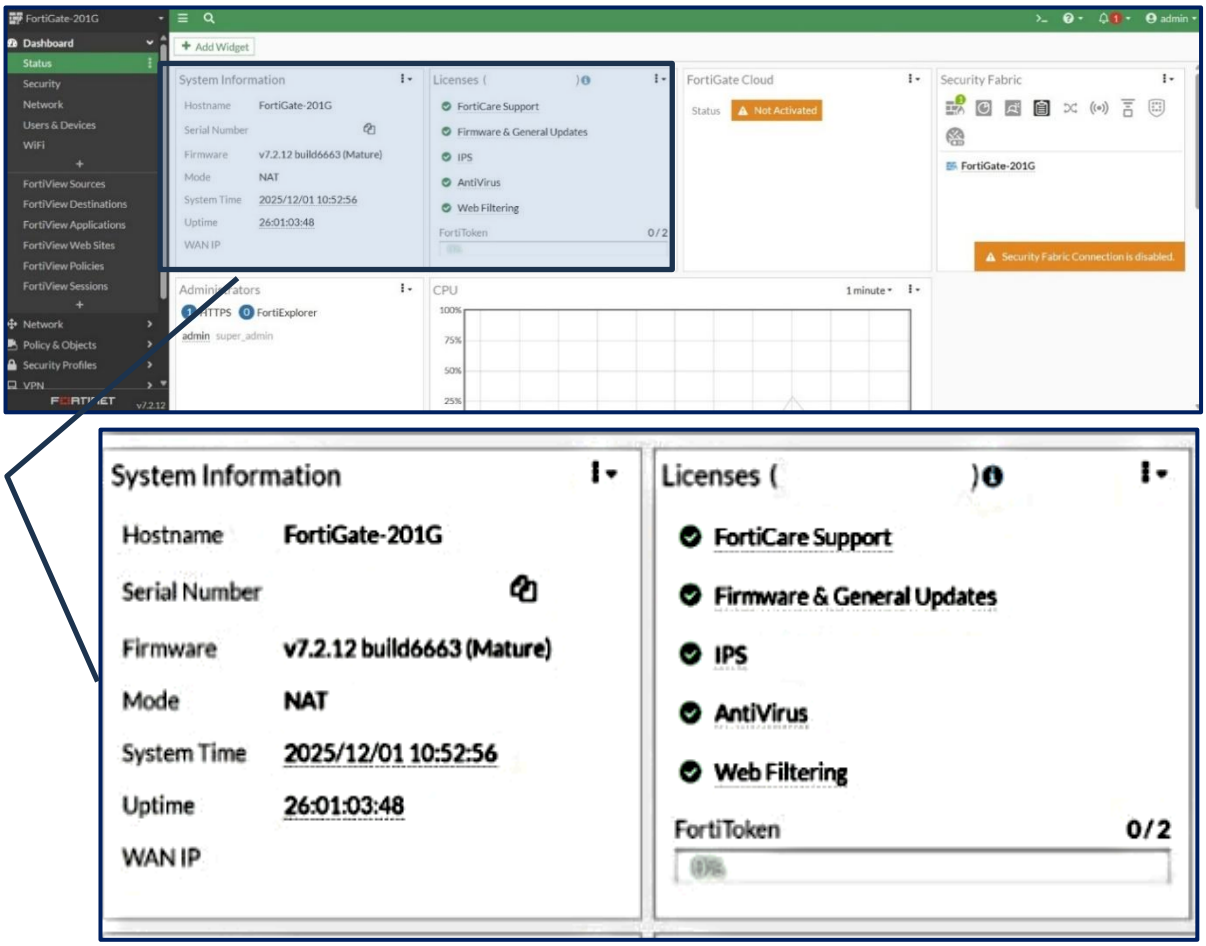




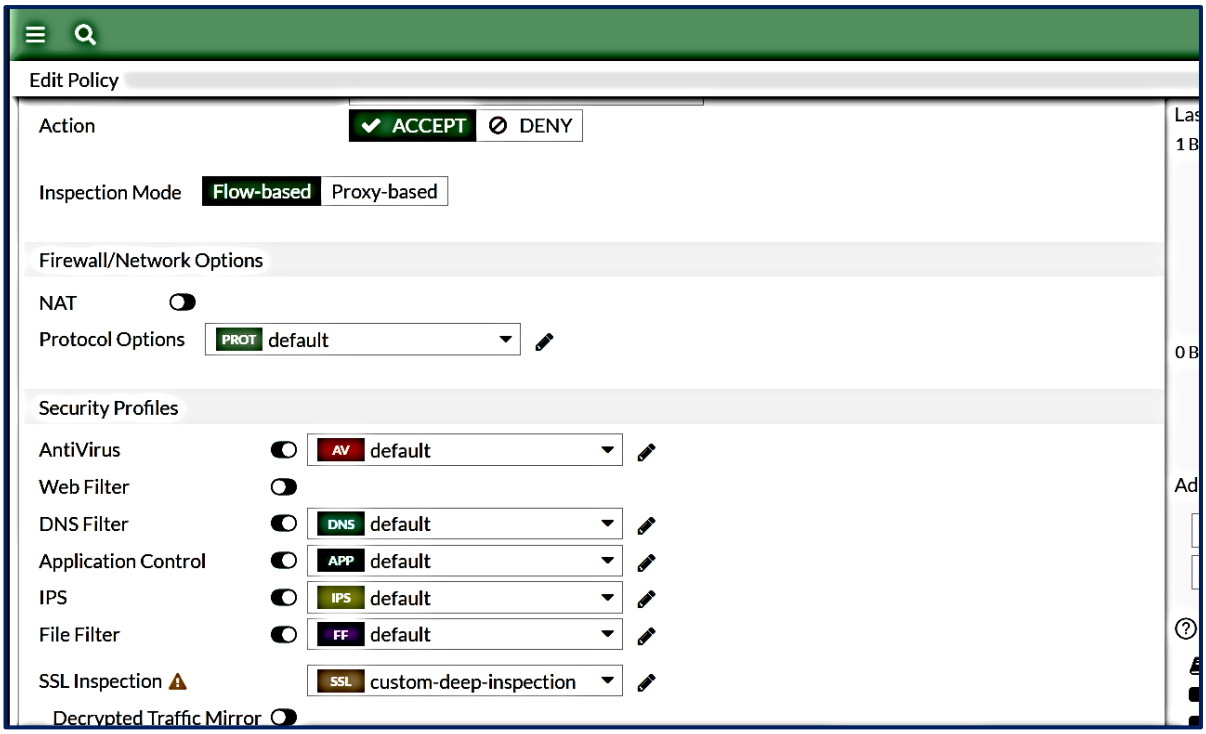
Decryption profile:



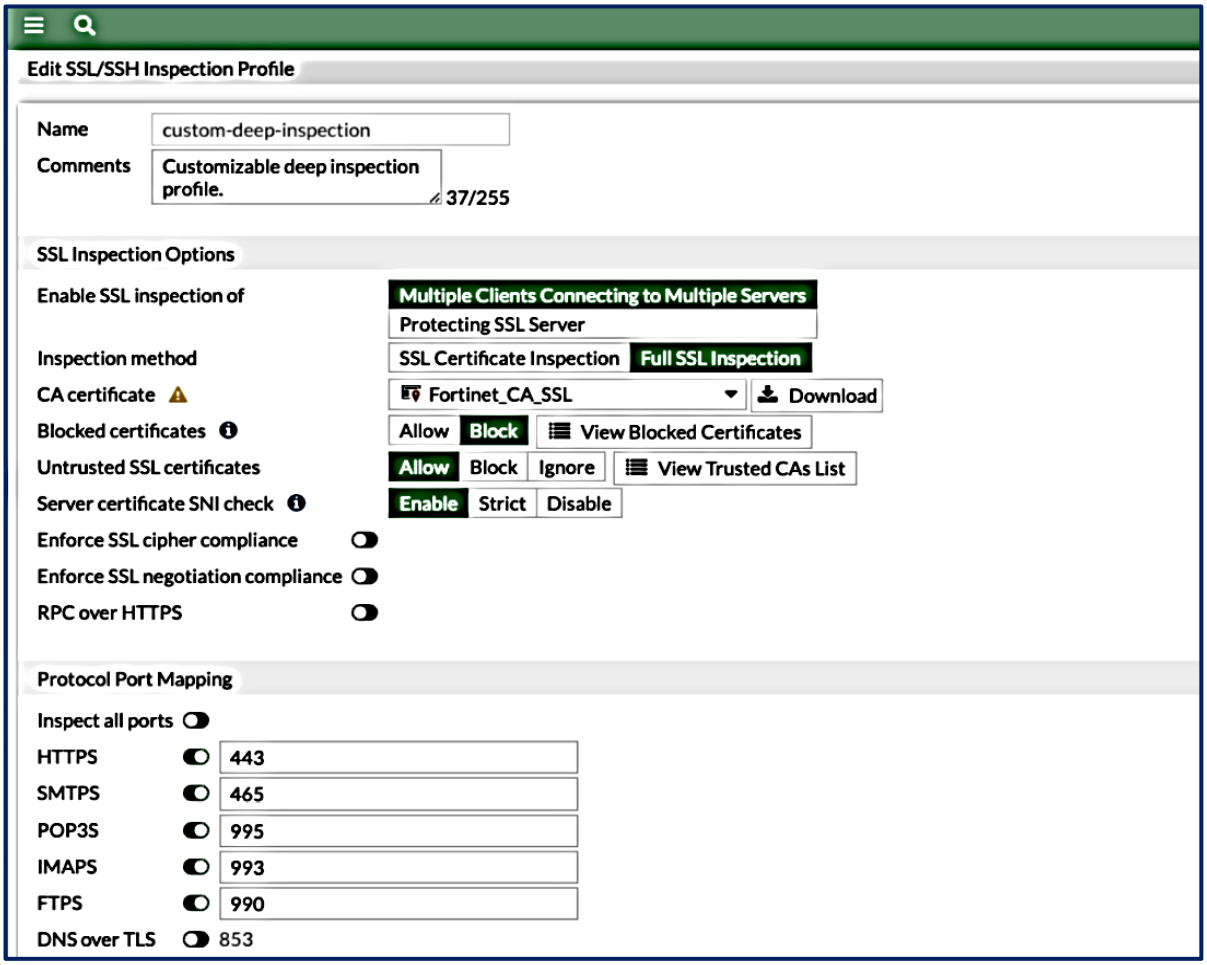
Fortinet Security Default configuration:



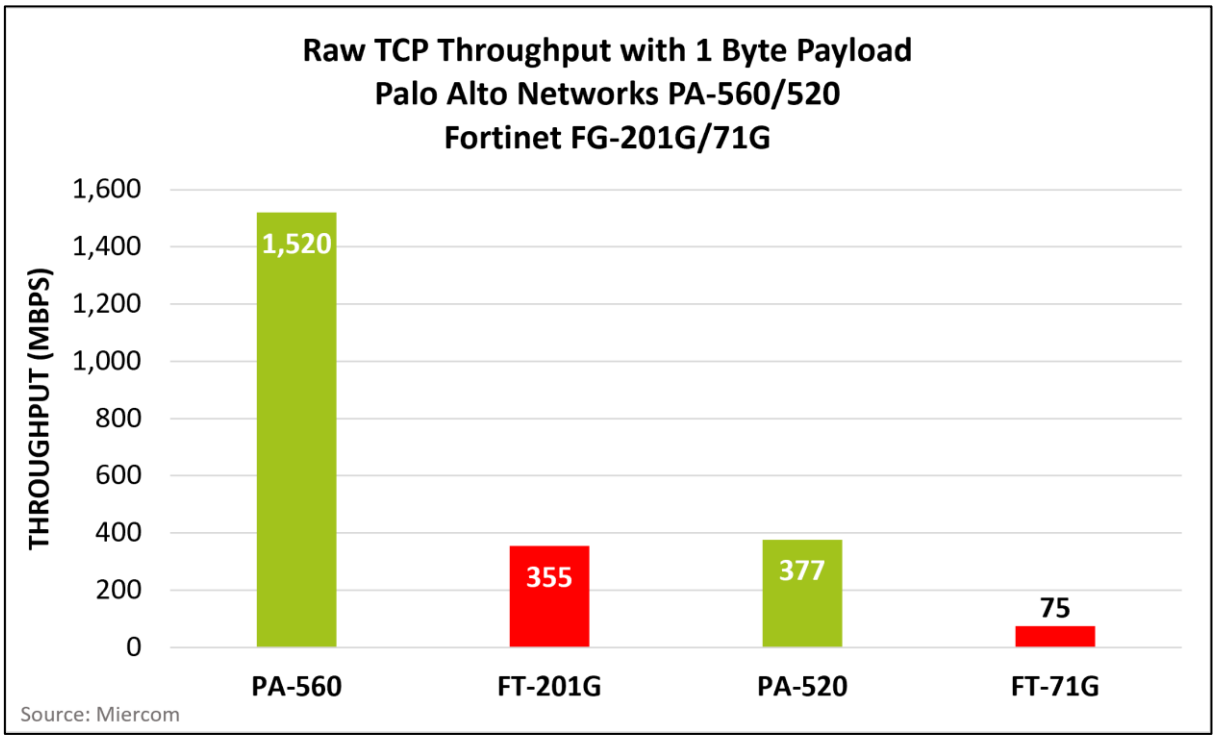
Flow based security configuration:



SSL Inspection (Forward Proxy):



5.1 Raw TCP Throughput (session sender profile)



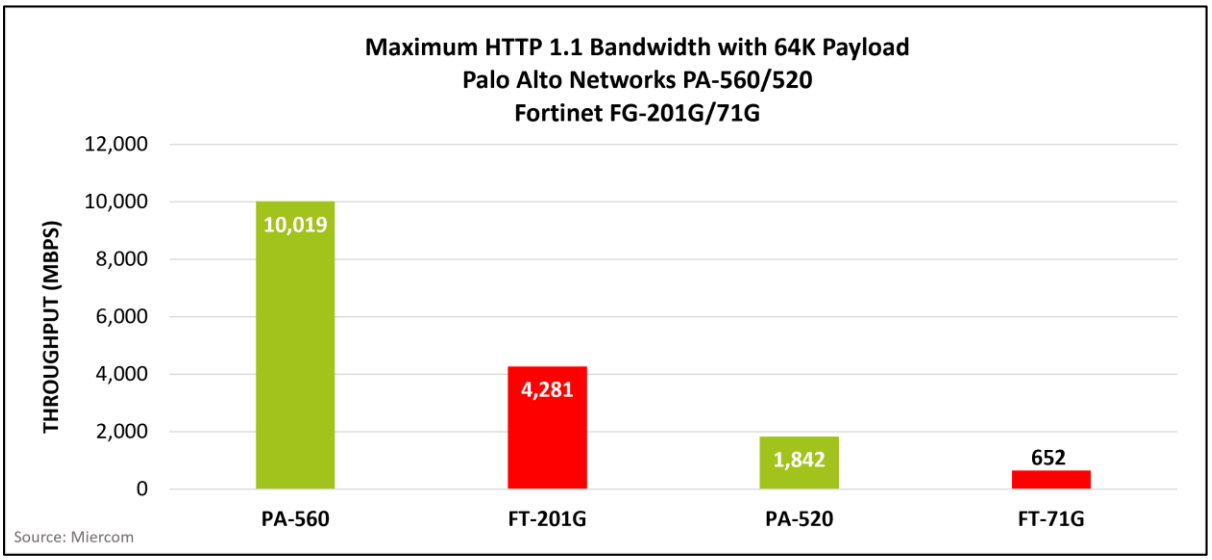
Palo Alto Networks PA-560 achieved a throughput of 1,520 Mbps, outperforming Fortinet FG-201G by more than 4×. The PA-520 recorded 377 Mbps, delivering over 5× higher throughput than the FG-71G, which reached just 75 Mbps. These results highlight consistent performance advantages for Palo Alto Networks platforms under identical test conditions with 1-byte payloads.

The Palo Alto Networks Advantage

Across both comparisons, Palo Alto Networks demonstrated 4–5X higher throughput versus Fortinet counterparts. The PA-560 sustained high throughput levels representative of enterprise-class processing efficiency, while the PA-520 maintained strong branch-level performance under identical testing. Fortinet's FG-201G and FG-71G fell significantly short in throughput, showing the efficiency of Palo Alto Networks' hardware acceleration and software optimization when processing small-packet traffic.

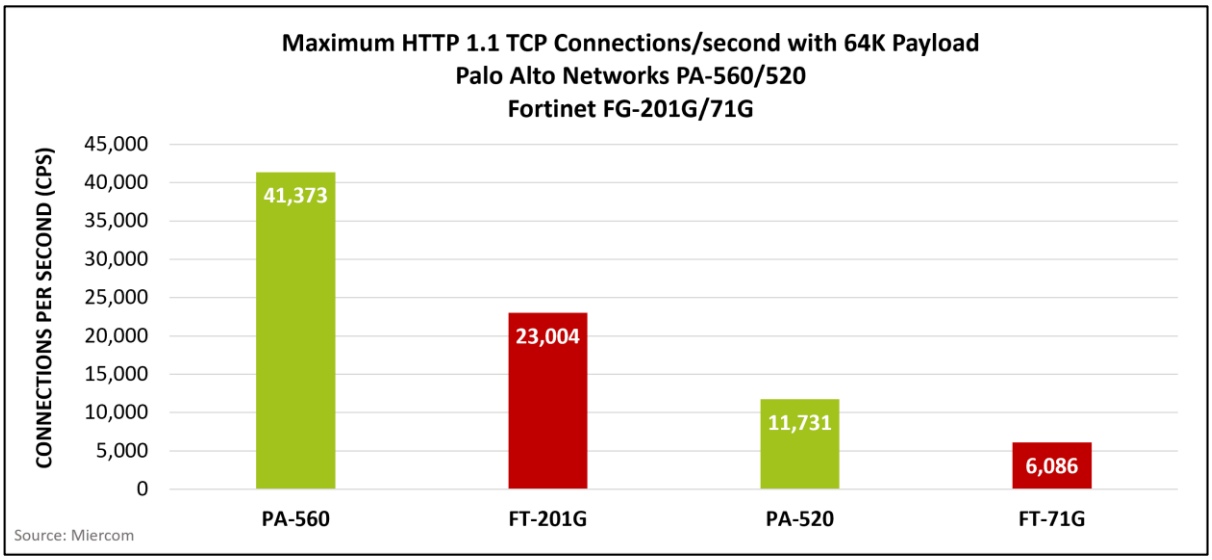
5.2 Maximum HTTP 1.1 Bandwidth & Connections per sec (CPS)

5.2.1 Bandwidth with 64K Payload (Mbps)



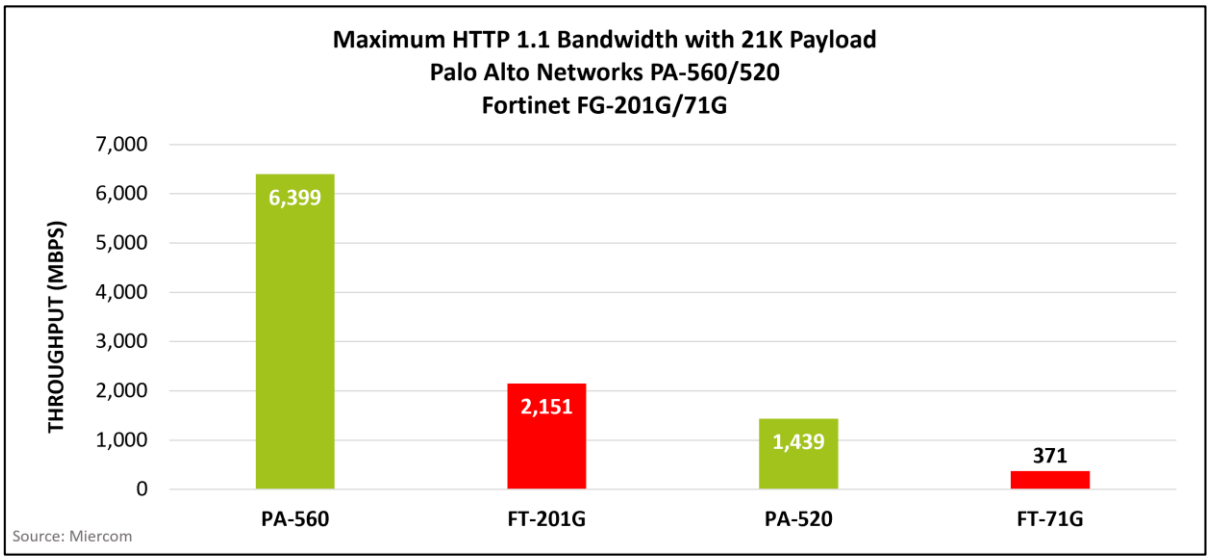
For a 64K payload, Palo Alto Networks PA-560 achieved 10,019 Mbps, more than 2.3 times higher than Fortinet FG-201G at 4,281 Mbps. The PA-520 reached 1,842 Mbps, outperforming the FG-71G at 652 Mbps by nearly 3 times. Palo Alto Networks appliances maintained strong high-throughput performance during large-payload HTTP testing, while the Fortinet models showed significantly reduced bandwidth efficiency.

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



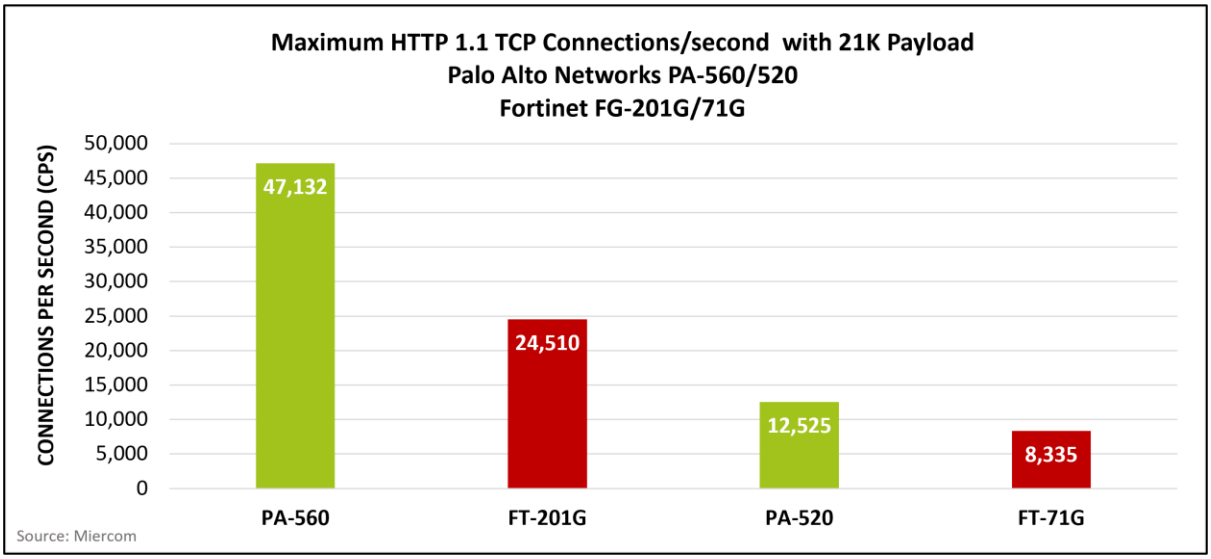
For a 64K payload, Palo Alto Networks PA-560 achieved 41,373 CPS, outperforming Fortinet FG-201G at 23,004 CPS by 80 percent. The PA-520 reached 11,731 CPS, while FG-71G measured 6,086 CPS, showing a 48 percent lower rate. Overall, Palo Alto Networks appliances demonstrated higher HTTP 1.1 connection handling under large-payload conditions compared to Fortinet models.

5.2.3 Bandwidth with 21K Payload (Mbps)



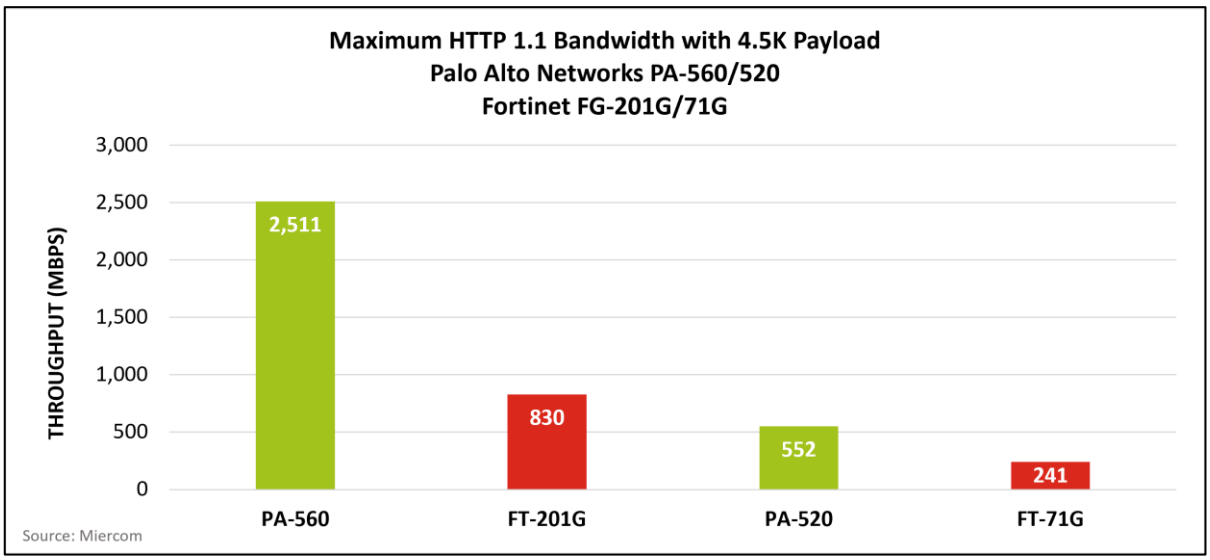
For a 21K payload, Palo Alto Networks PA-560 reached 6,399 Mbps, delivering nearly 3 times the throughput of Fortinet FG-201G at 2,151 Mbps. The PA-520 achieved 1,439 Mbps, outperforming the FG-71G at 371 Mbps by almost 4 times. These results show consistent high-bandwidth efficiency for Palo Alto Networks appliances during HTTP 1.1 testing, while Fortinet models demonstrated lower throughput under the same conditions.

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



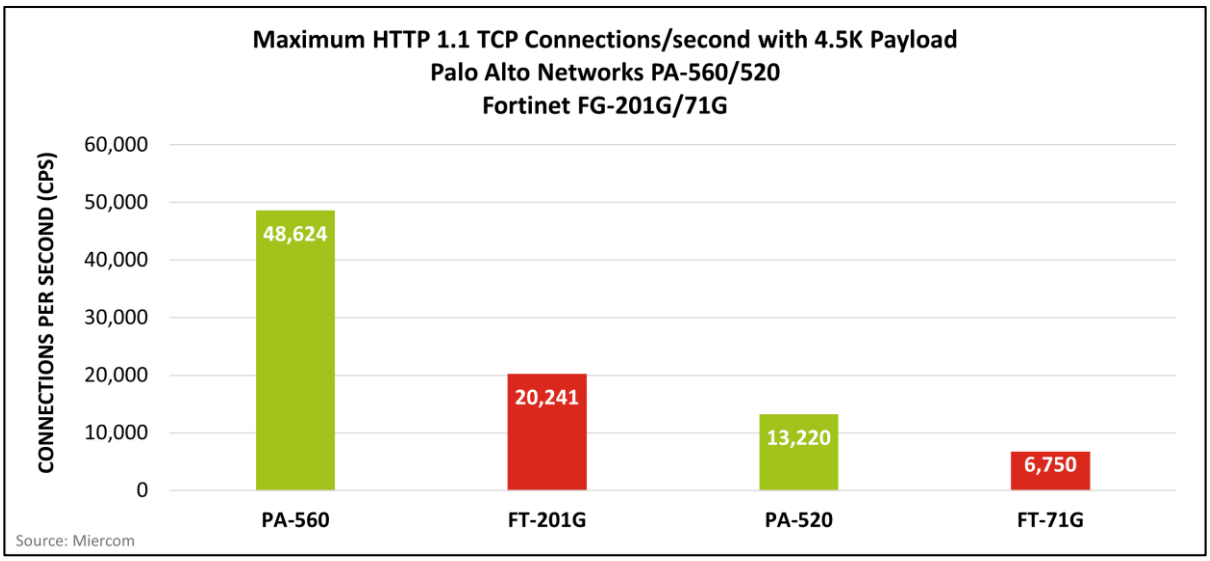
For a 21K payload, Palo Alto Networks PA-560 reached 47,132 CPS, 92 percent higher than Fortinet FG-201G at 24,510 CPS. The PA-520 recorded 12,525 CPS, surpassing FG-71G at 8,335 CPS by 50 percent. Palo Alto Networks appliances maintained strong performance consistency across medium payload sizes, while Fortinet devices operated at significantly lower rates.

5.2.5 Bandwidth with 4.5K Payload (Mbps)



For a 4.5K payload, Palo Alto Networks PA-560 achieved 2,511 Mbps, which is more than 3 times the throughput of Fortinet FG-201G at 830 Mbps. The PA-520 reached 552 Mbps, outperforming the FG-71G at 241 Mbps by more than 2 times. These results show that Palo Alto Networks appliances deliver stronger HTTP 1.1 performance with medium payload sizes, while Fortinet models exhibited noticeably lower throughput under the same test conditions.

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



For a 4.5K payload, Palo Alto Networks PA-560 achieved 48,624 CPS, exceeding Fortinet FG-201G at 20,241 CPS by 140 percent. The PA-520 delivered 13,220 CPS, nearly doubling FG-71G at 6,750 CPS. These results indicate that Palo Alto Networks maintained superior connection performance across smaller payload sizes compared with Fortinet appliances.

The Palo Alto Networks Advantage

Palo Alto Networks continued to demonstrate superior efficiency and consistency compared to Fortinet across all payload sizes. In both bandwidth and connection rate tests, Palo Alto Networks appliances exhibited minimal degradation when services were enabled, while Fortinet appliances showed significantly higher performance loss.

64K Payload

For bandwidth, Palo Alto Networks PA-560 and PA-520 maintained strong throughput performance, showing minimal decline when services were enabled, averaging 3% loss. Fortinet FG-201G and FG-71G dropped by an average of 5%. For connection rate, Palo Alto Networks sustained high performance with only minor change. Fortinet models achieved lower rates overall, averaging 45% less throughput compared to Palo Alto Networks under identical conditions.

21K Payload

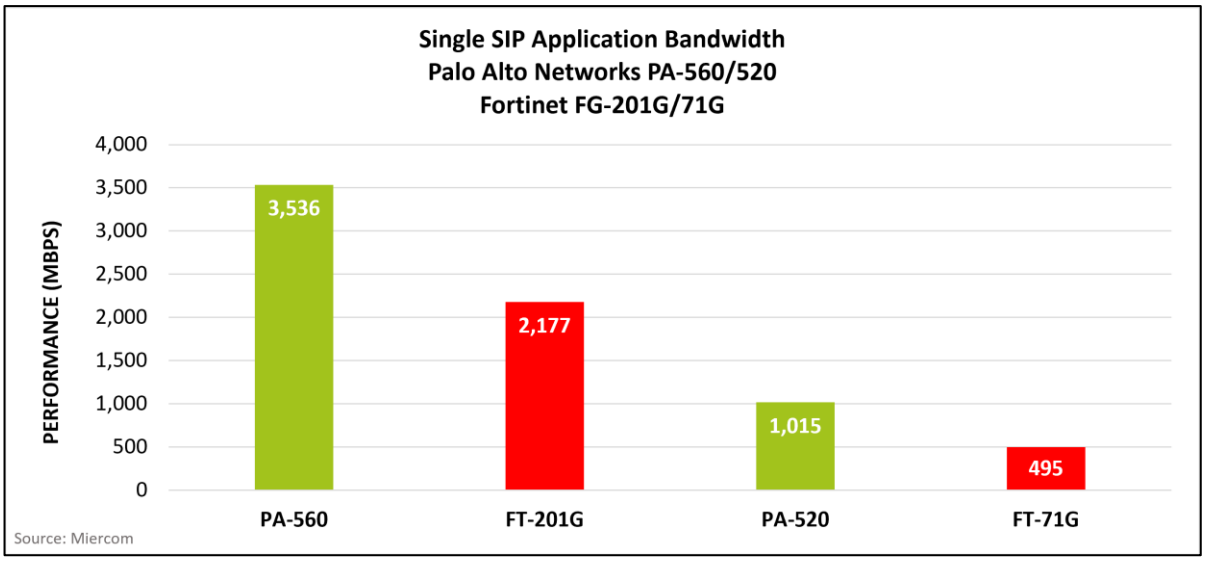
For bandwidth, Palo Alto Networks appliances demonstrated stable performance with roughly 6% average degradation when services were enabled. Fortinet appliances saw an average reduction of 8%. In connection rate testing, Palo Alto Networks held a 92% higher connection rate than Fortinet on average, showing consistent efficiency under medium payload sizes.

4.5K Payload

For bandwidth, Palo Alto Networks averaged a 5% performance decrease when services were enabled, while Fortinet appliances experienced a 10% loss. For connection rate, Palo Alto Networks maintained up to 140% higher performance than Fortinet, confirming consistent responsiveness even under smaller payload conditions.

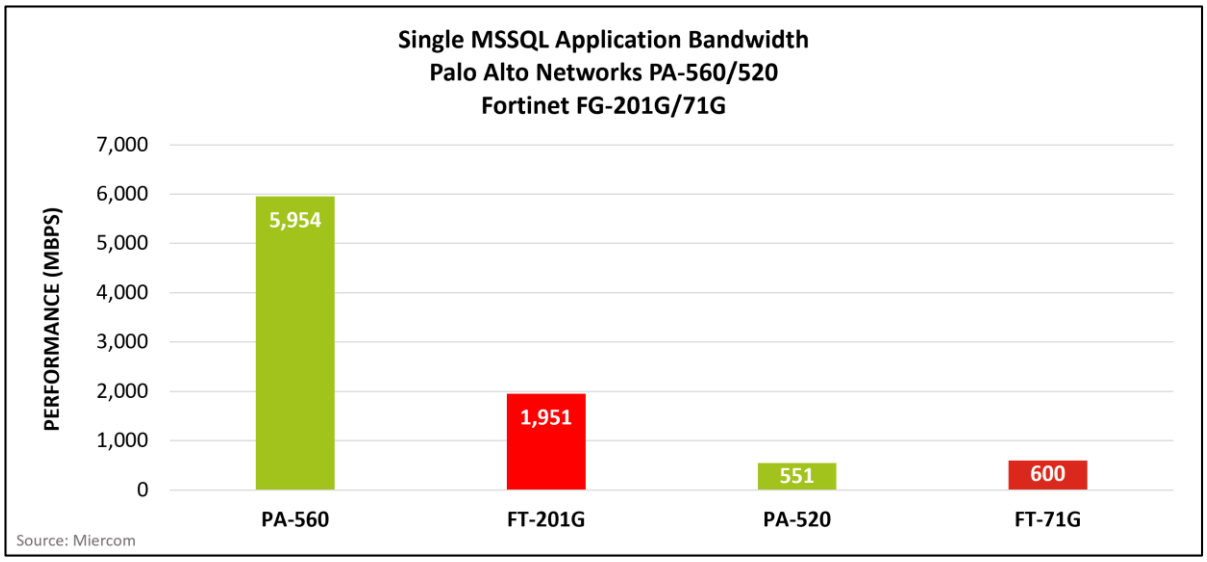
5.3 Single Application Bandwidth

5.3.1 Session initiation Protocol (SIP) Application Bandwidth



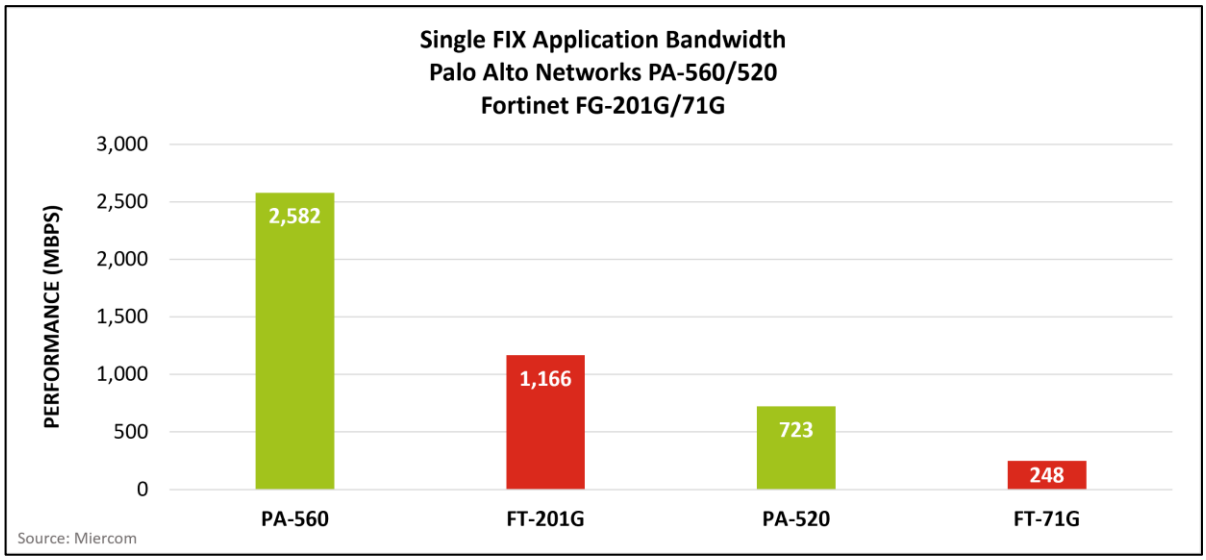
For Single SIP Application bandwidth, Palo Alto Networks appliances delivered substantially higher performance than the Fortinet models under identical conditions. PA-560 reached 3,536 Mbps, providing 1.6 times the bandwidth of Fortinet FG-201G at 2,177 Mbps. PA-520 achieved 1,015 Mbps, offering just over 2 times the throughput of Fortinet FG-71G at 495 Mbps. Across both model tiers, Palo Alto Networks maintained a clear advantage, with consistently higher application bandwidth than the comparable Fortinet appliances.

5.3.2 MSSQL Application Bandwidth



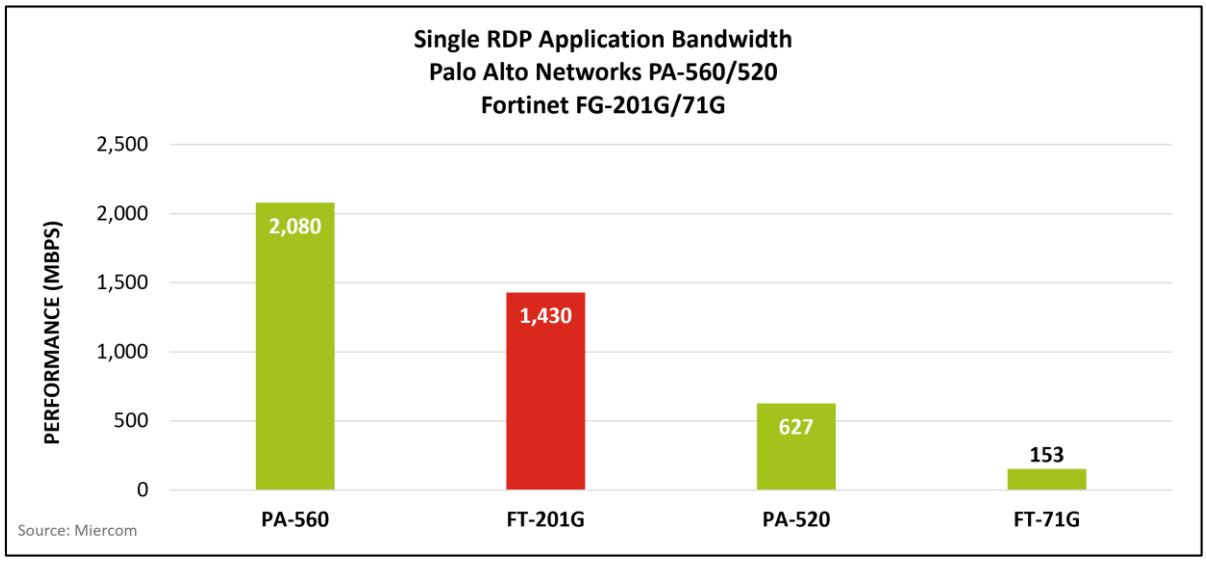
For Single MSSQL Application bandwidth, Palo Alto Networks sustained significantly higher throughput than Fortinet across both appliance tiers. The PA-560 reached 5,954 Mbps, compared to the FG-201G at 1,951 Mbps. In the mid-range tier, the PA-520 delivered 551 Mbps while the FG-71G measured 600 Mbps. Across all measured MSSQL tests, Palo Alto Networks maintained the strongest overall performance at the upper tier with substantial throughput headroom for real-world database workloads.

5.3.3 Financial Information eXchange (FIX) Application Bandwidth



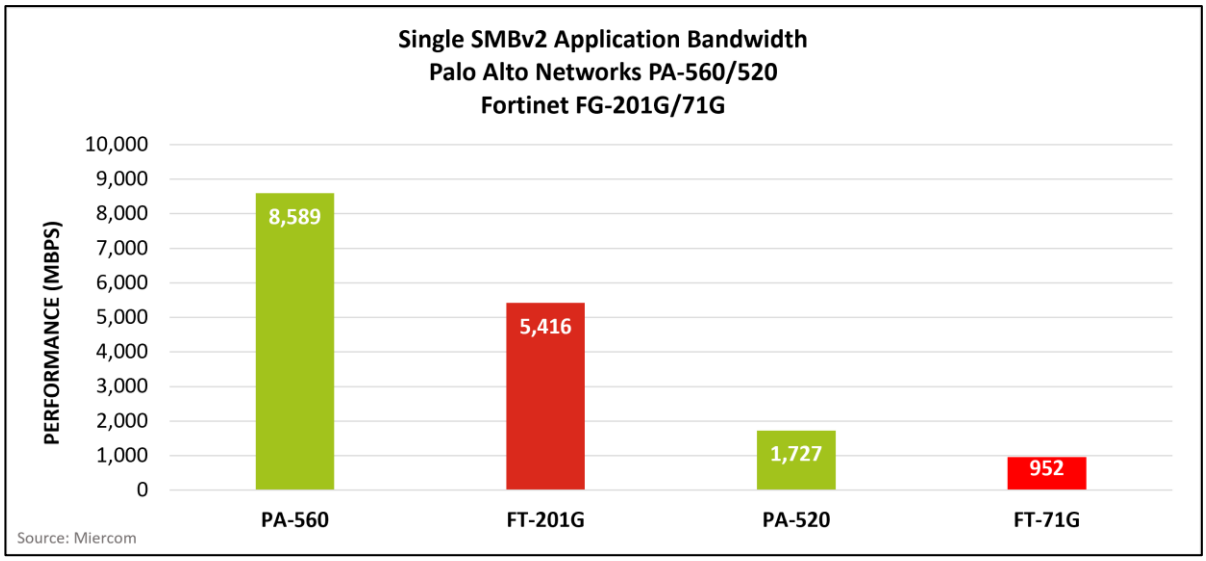
For Single FIX Application bandwidth, Palo Alto Networks continued to deliver higher performance across both appliance tiers. The PA-560 reached 2,582 Mbps, more than double the throughput of Fortinet FG-201G at 1,166 Mbps. In the mid-range class, PA-520 achieved 723 Mbps compared to Fortinet FG-71G at 248 Mbps, giving Palo Alto Networks nearly three times the performance. Across both tiers tested, Palo Alto Networks sustained a clear advantage in FIX application throughput.

5.3.4 Remote Desktop Protocol (RDP) Application Bandwidth



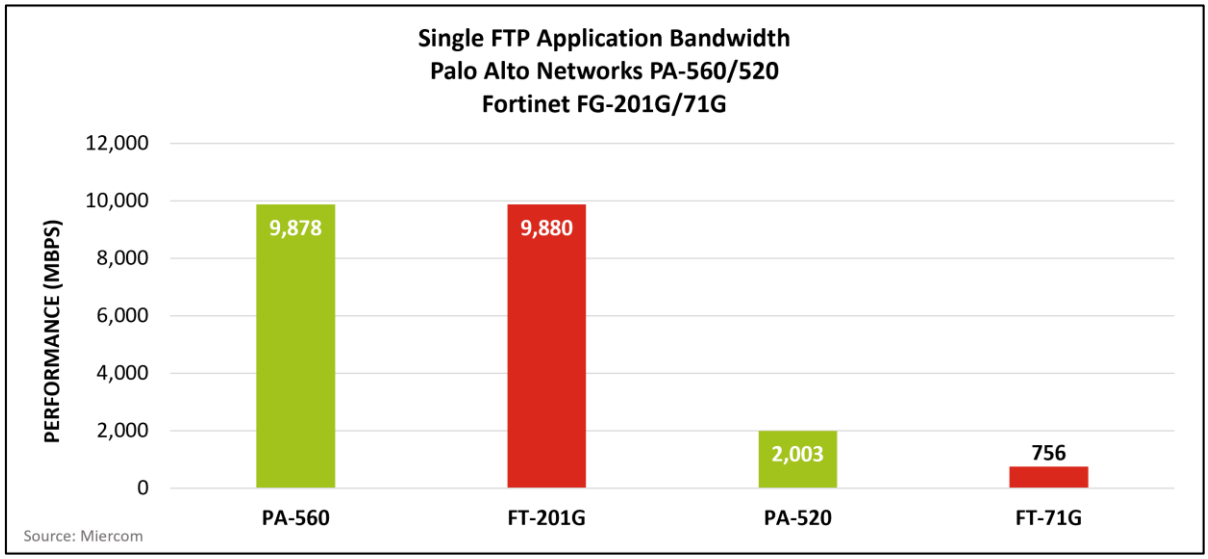
For Single RDP Application bandwidth, Palo Alto Networks delivered consistently higher throughput across both appliance tiers. The PA-560 achieved 2,080 Mbps, surpassing Fortinet FG-201G at 1,430 Mbps. In the mid-range tier, PA-520 reached 627 Mbps, compared to FG-71G at 153 Mbps, giving Palo Alto Networks more than four times the performance. Across all measured RDP application tests, Palo Alto Networks maintained a clear lead in bandwidth.

5.3.5 Server Message Block 2 (SMBv2) Application Bandwidth



For Single SMBv2 Application bandwidth, Palo Alto Networks delivered substantially higher throughput across both appliance tiers. The PA-560 reached 8,589 Mbps, outperforming Fortinet's FG-201G at 5,416 Mbps. In the mid-range tier, the PA-520 measured 1,727 Mbps, compared to the FG-71G at 952 Mbps. Across all measured SMBv2 application tests, Palo Alto Networks demonstrated consistently stronger bandwidth performance.

5.3.6 File Transfer Protocol (FTP) Application Bandwidth



For Single FTP Application bandwidth, throughput remained high for both vendors' top-tier models, with the PA-560 at 9,878 Mbps and the FG-201G close behind at 9,880 Mbps. In the mid-range tier, however, the PA-520 delivered 2,003 Mbps, significantly higher than the FG-71G at 756 Mbps. Across the full set of FTP application tests, Palo Alto Networks maintained a bandwidth advantage in the mid-range appliance class.

The Palo Alto Networks Advantage

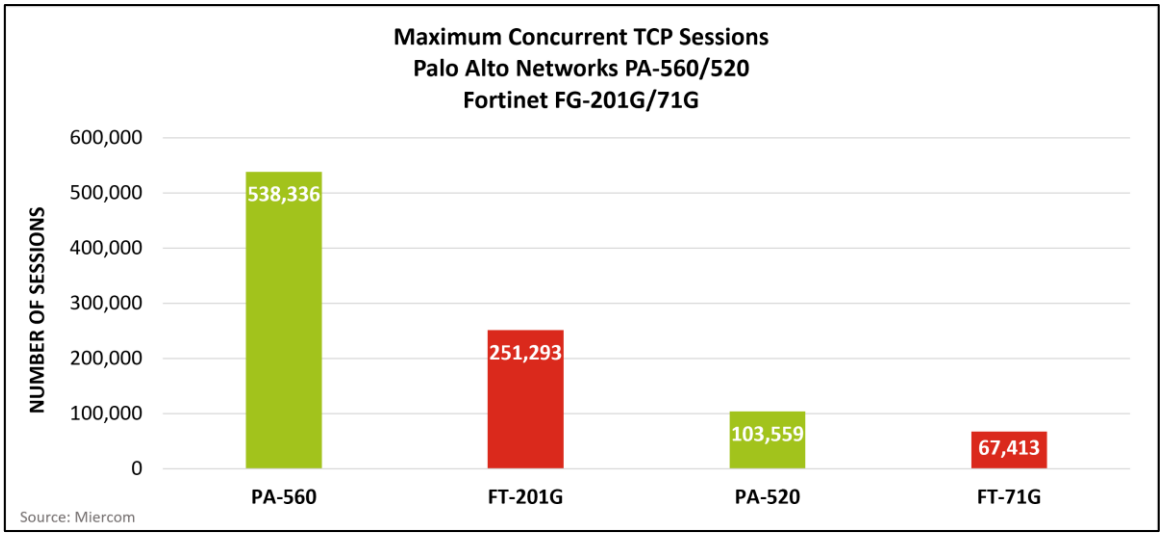
Fortinet platforms continued to exhibit significant limitations across several real-world application tests. As in the prior tests, Fortinet appliances were unable to process FIX traffic, resulting in 100% traffic loss. In addition, Fortinet platforms delivered very low throughput for SIP and MSSQL protocols, making them unsuitable for environments that rely on these latency-sensitive or transaction-heavy applications.

When evaluating broader enterprise workflows — including RDP, SMBv2, and FTP — Fortinet appliances showed substantial performance degradation, particularly in the mid-range tier, where bandwidth output dropped sharply compared to Palo Alto Networks.

The Palo Alto Networks PA-500 series, by contrast, reliably processed all six real-world applications tested, maintaining consistent and predictable performance even with security services enabled. Across SIP, MSSQL, FIX, RDP, SMBv2, and FTP, Palo Alto Networks demonstrated robust application handling and significantly higher throughput, making it the more dependable platform for mixed-application enterprise environments.

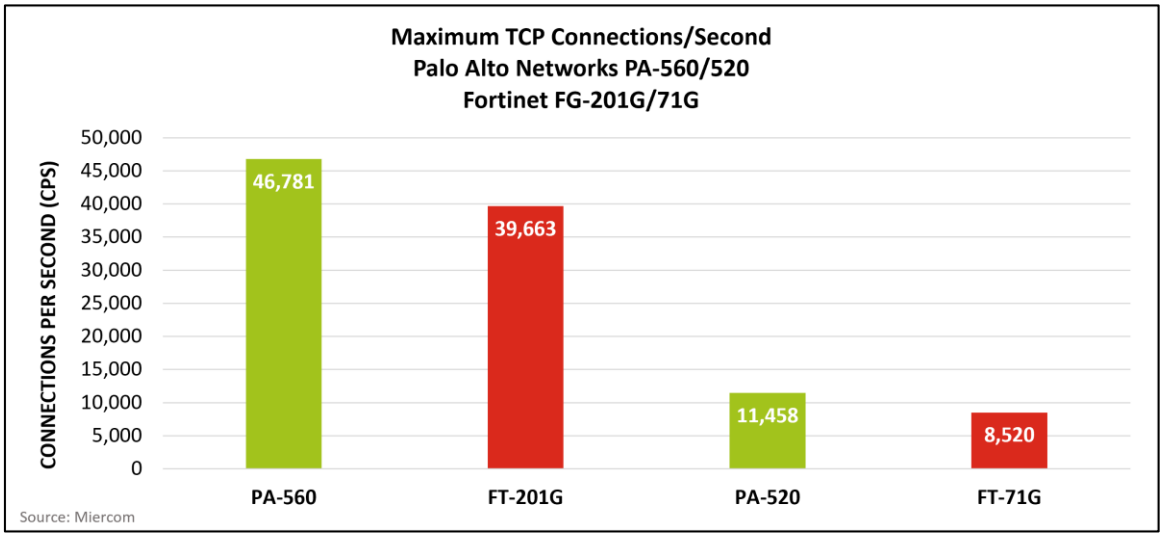
5.4 TCP Maximum Capacity

5.4.1 Maximum Concurrent TCP Sessions



Palo Alto Networks PA-500 Series sustained higher maximum concurrent TCP sessions than the Fortinet platforms across both appliance tiers. The PA-560 maintained the highest session capacity overall, followed by the PA-520, while the FG-201G and FG-71G trailed with substantially lower limits.

5.4.2 Maximum TCP Connections/sec (CPS)

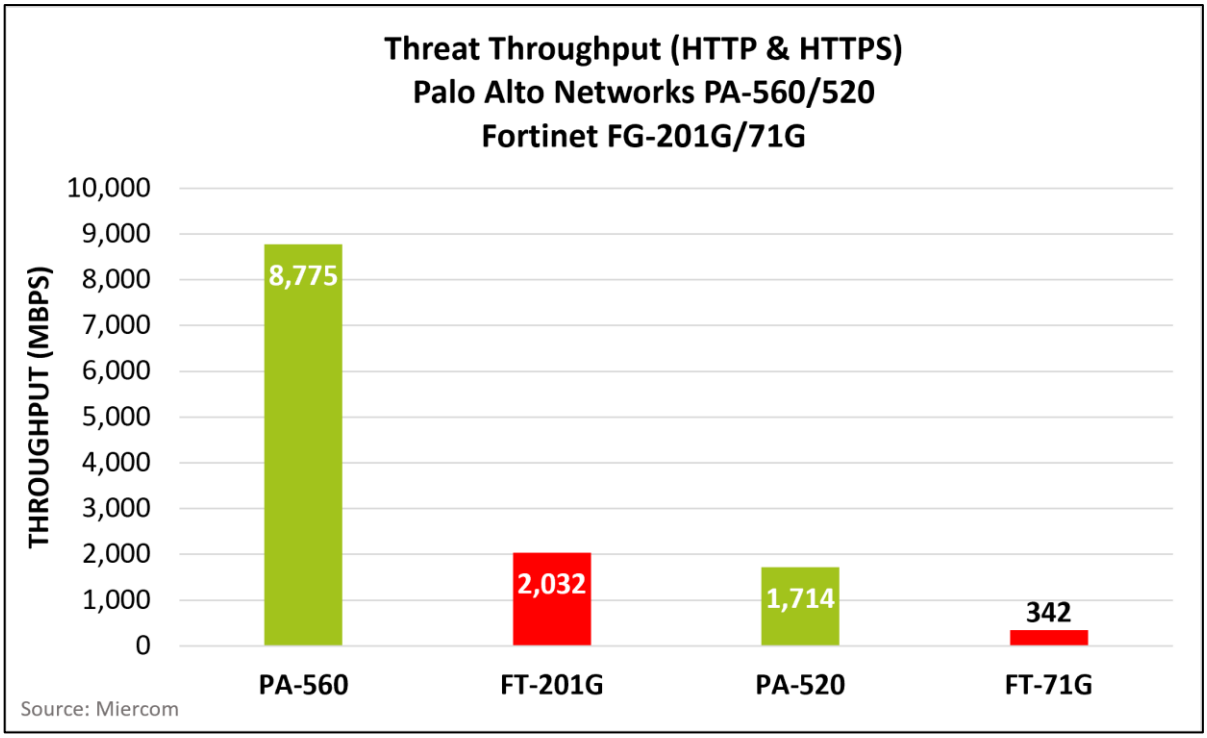


Palo Alto Networks PA-500 Series achieved higher TCP connection rates per second than the comparable Fortinet platforms. The PA-560 delivered the top CPS performance, with the PA-520 close behind, while the FG-201G and FG-71G showed significantly lower connection-handling capability.

The Palo Alto Networks Advantage

Palo Alto Networks appliances demonstrated higher TCP session capacity across both platforms. The PA-560 sustained more than twice the concurrent TCP sessions of the FG-201G, and the PA-520 held a clear lead over the FG-71G. For connection rate, both Palo Alto Networks platforms maintained higher CPS performance, with the PA-560 exceeding the FG-201G and the PA-520 outperforming the FG-71G. The results show consistent TCP scalability for Palo Alto Networks under full security services.

5.5 Enterprise Traffic Mix (HTTP & HTTPS)

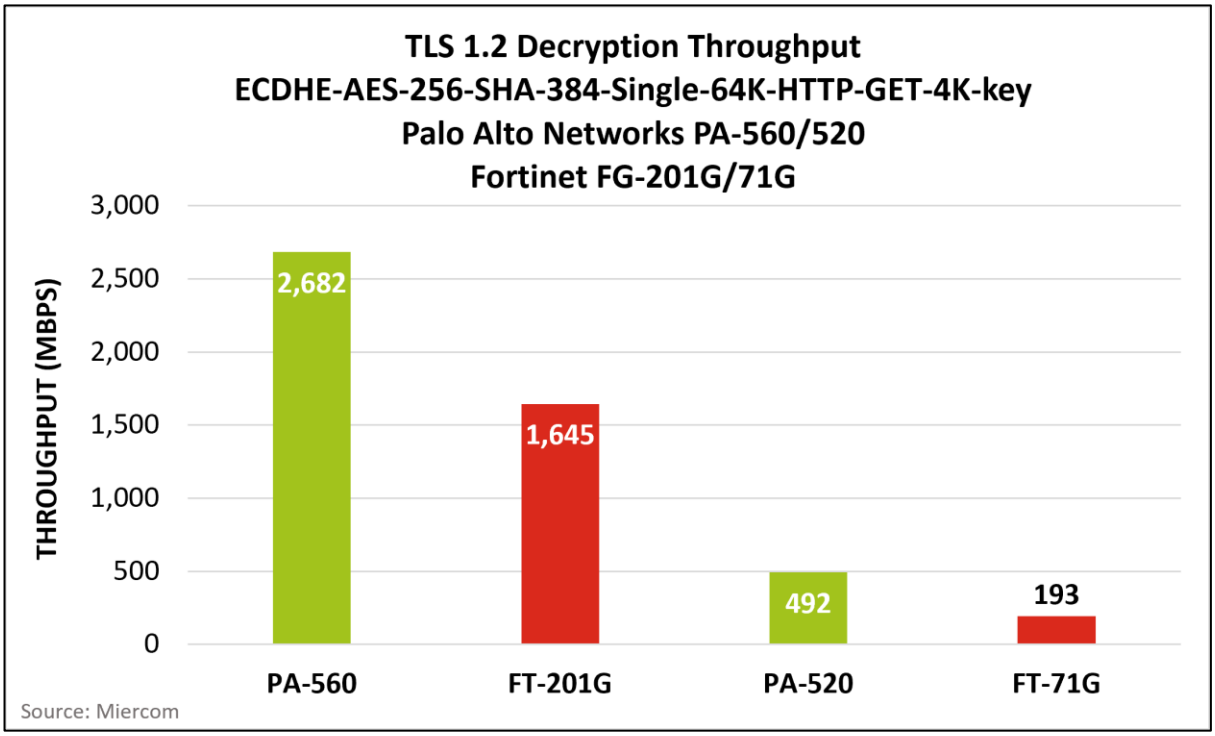


The PA-560 delivered more than four times the HTTP and HTTPS connection rate of the FG-201G, while the PA-520 outperformed the FG-71G by a wide margin. Palo Alto Networks maintained higher throughput across both platforms.

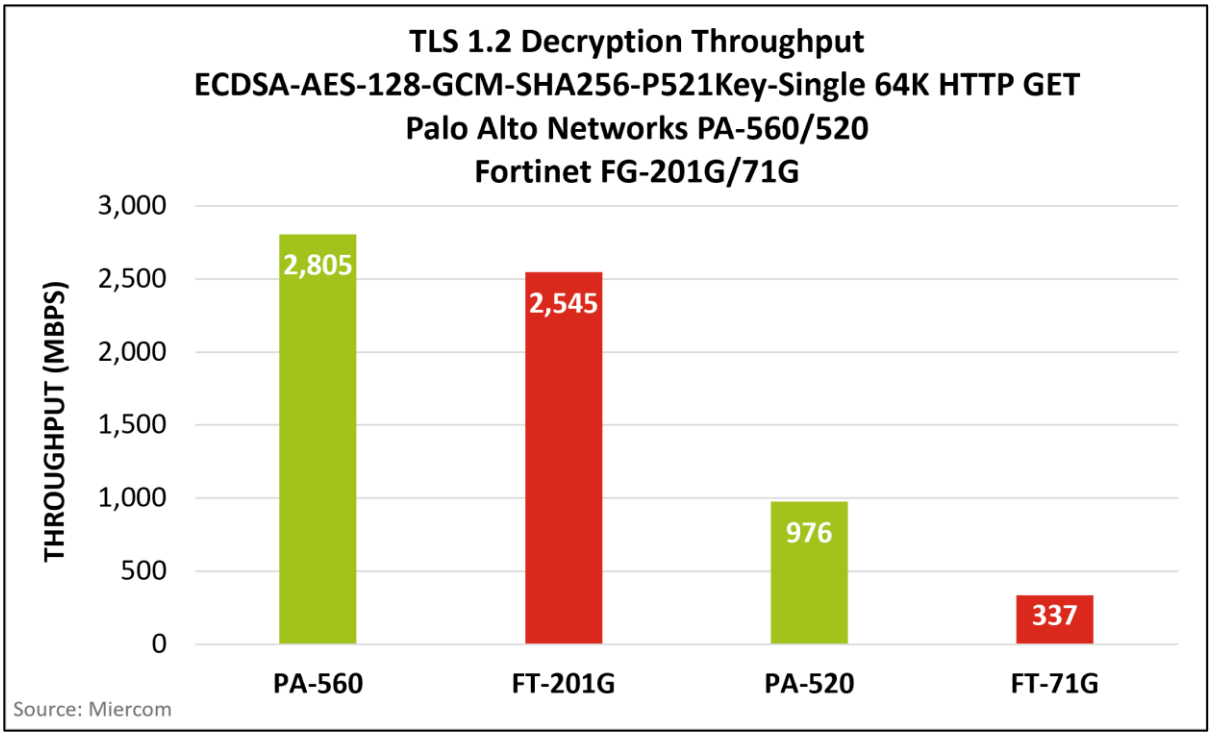
The Palo Alto Networks Advantage

Palo Alto Networks showed higher performance for mixed HTTP and HTTPS traffic. The PA-560 established more connections per second than the FG-201G, and the PA-520 exceeded the connection rate of the FG-71G. The results reflect stronger traffic handling and more consistent performance under full security services.

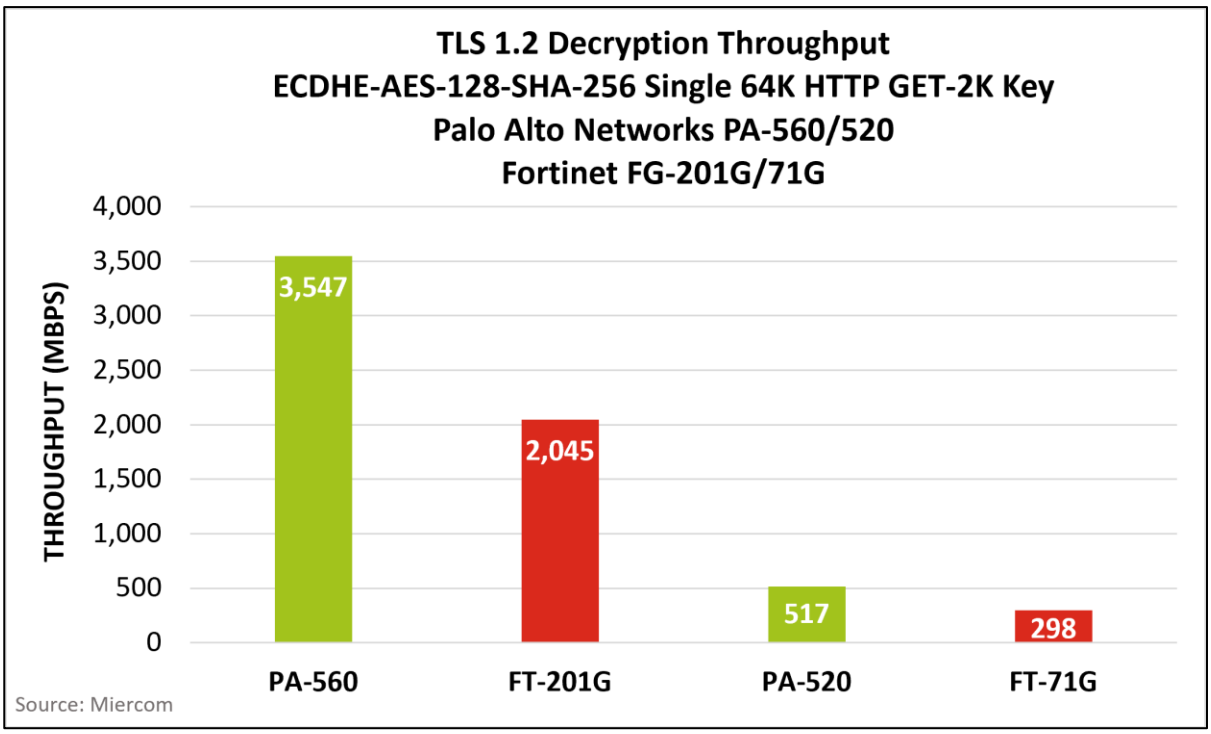
5.6 Decryption Throughput Analysis



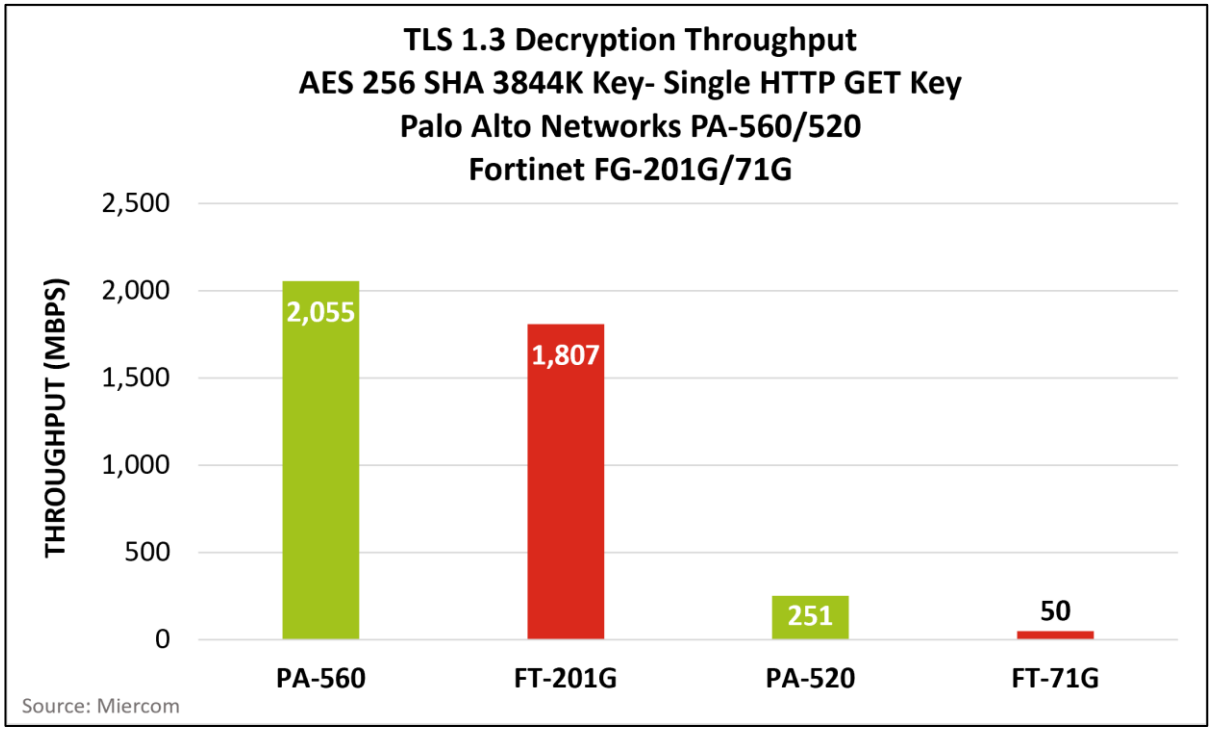
Palo Alto Networks delivered the highest TLS 1.2 decryption throughput with the PA-560 reaching 2,682 Mbps, outperforming the Fortinet FG-201G at 1,645 Mbps. The PA-520 also exceeded the FG-71G, showing stronger performance across both performance tiers.



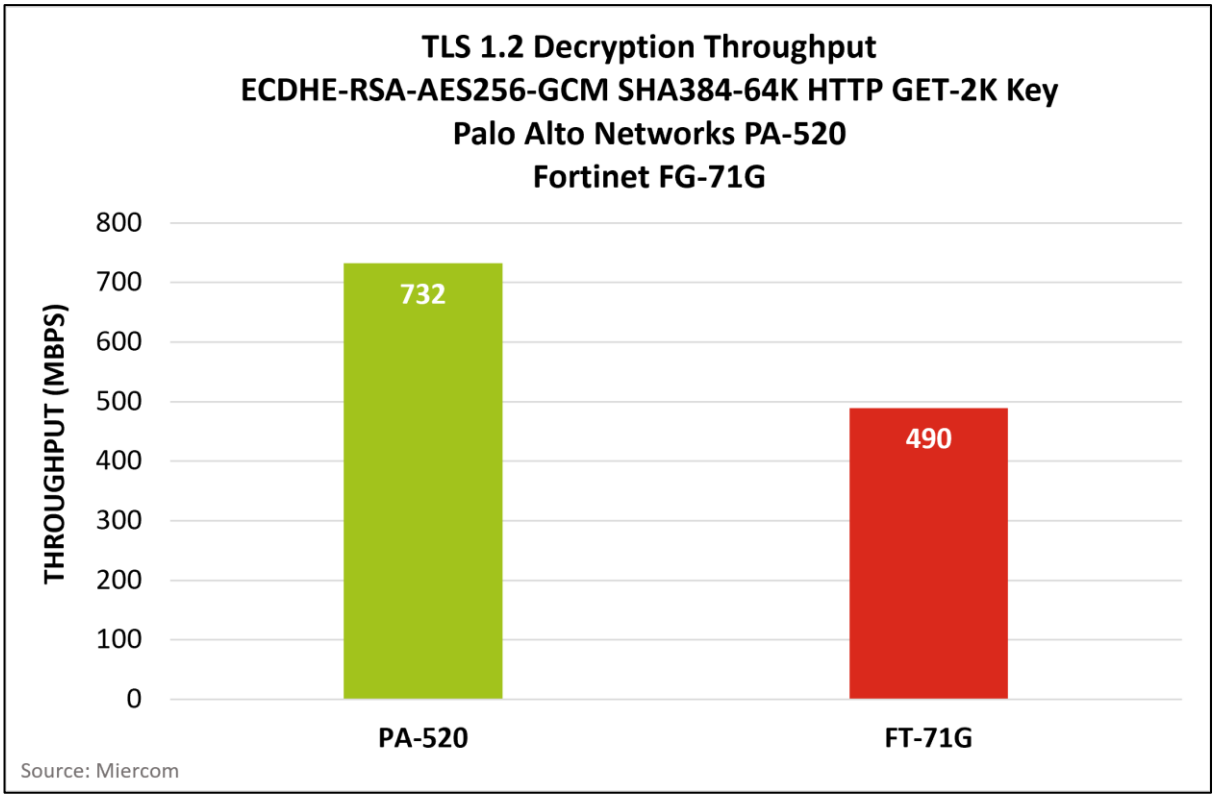
The PA-560 led with 2,805 Mbps, maintaining a decisive margin over the FG-201G at 2,545 Mbps. The PA-520 also remained ahead of the FG-71G, underscoring consistent performance advantages in ECDSA-based decryption.



Palo Alto Networks again held a strong lead, with the PA-560 achieving 3,547 Mbps, significantly higher than the FG-201G's 2,045 Mbps. In the mid-range, the PA-520 outperformed the FG-71G by a wide margin.



The PA-560 reached 2,055 Mbps in TLS 1.3 decryption throughput, compared to 1,807 Mbps on the FG-201G. The PA-520 delivered nearly 5× the throughput of the FG-71G, demonstrating stronger performance under TLS 1.3 encryption.



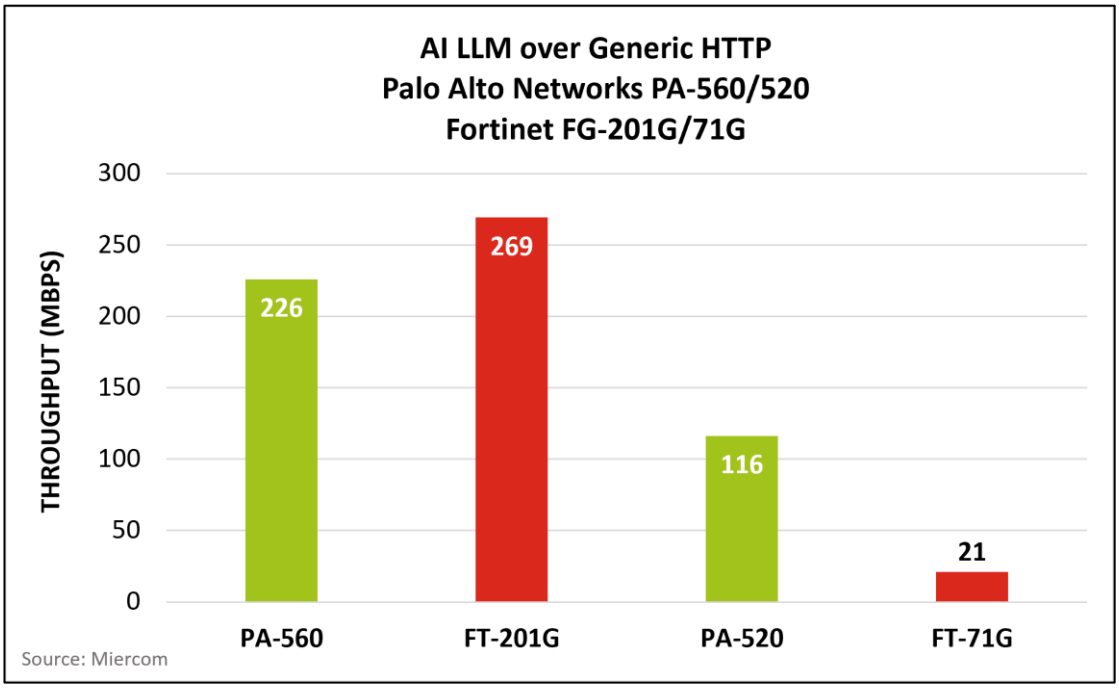
In RSA-based TLS 1.2 decryption, the PA-520 achieved 732 Mbps, outperforming the FG-71G at 490 Mbps, reflecting Palo Alto Networks' better handling of compute-intensive RSA operations.

The Palo Alto Networks Advantage

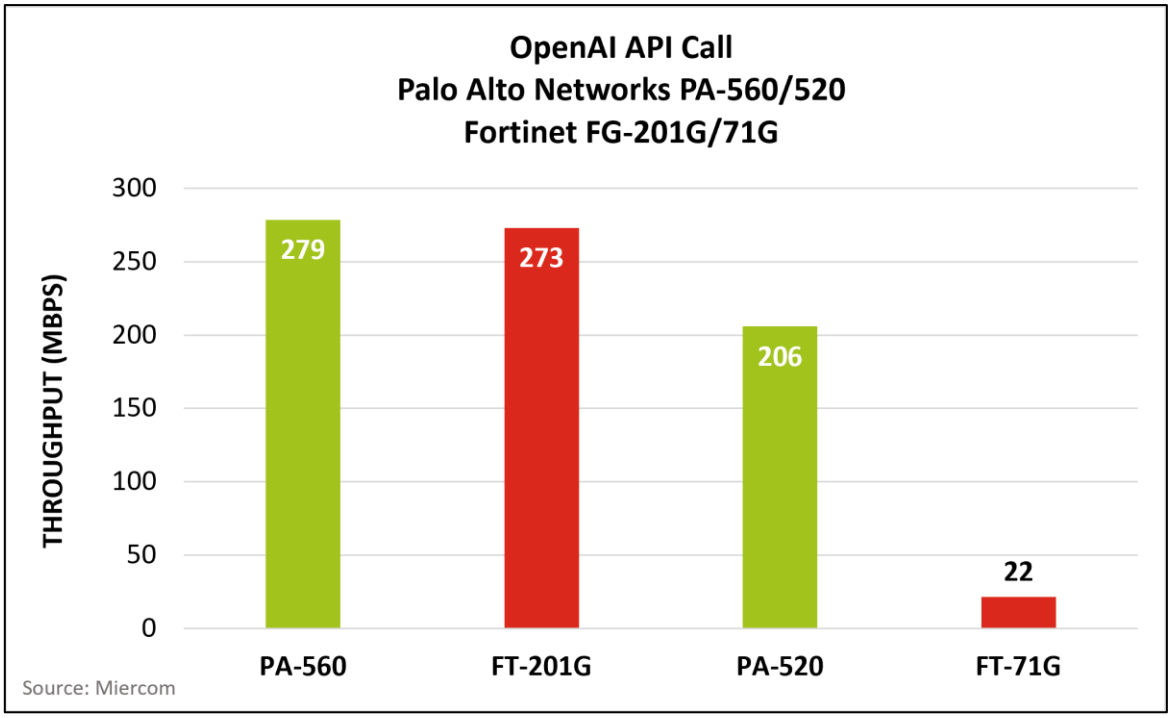
Across all TLS 1.2 and TLS 1.3 decryption scenarios, Palo Alto Networks consistently demonstrated higher throughput than the comparable Fortinet models. The PA-560 outperformed the FG-201G in every cipher suite tested, while the PA-520 delivered substantially better results than the FG-71G, often by wide margins. These results highlight Palo Alto Networks stronger encrypted traffic processing efficiency and its ability to maintain higher performance under modern, compute-heavy TLS workloads.

5.7 AI and LLM Traffic Performance (The Next Generation of Enterprise Traffic)

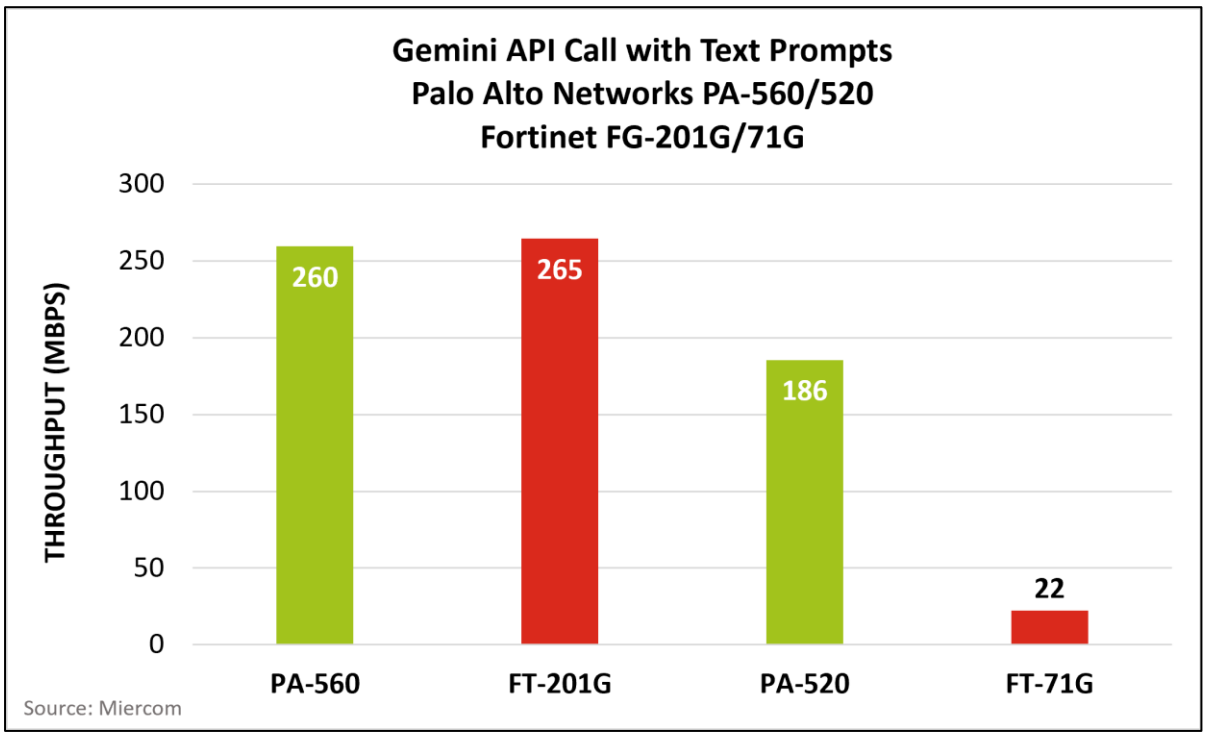
5.7.1 LLM Text Workflows



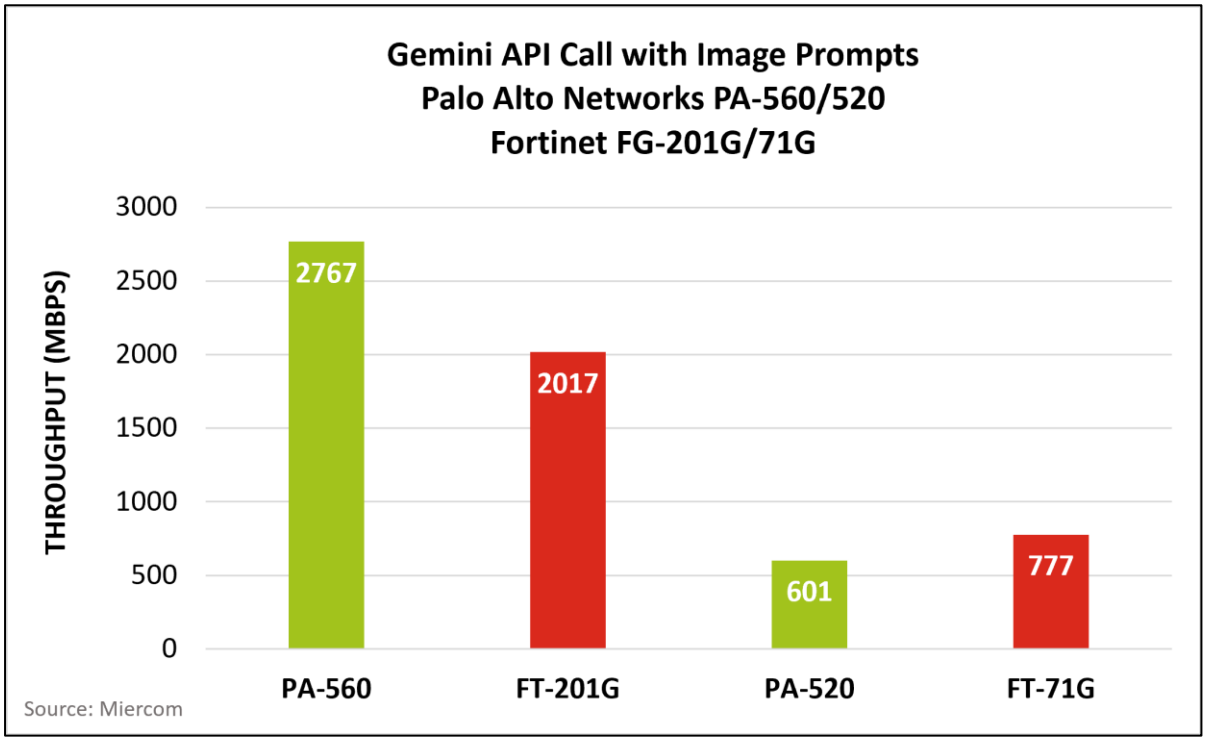
For generic HTTP traffic carrying LLM requests, Fortinet FG-201G achieved the highest throughput at 269 Mbps, followed by Palo Alto Networks PA-560 at 226 Mbps. In the mid-range tier, PA-520 sustained 116 Mbps, which was more than 5× the 21 Mbps measured for Fortinet FG-71G, indicating a substantial gap in AI-related HTTP capacity at the entry level.



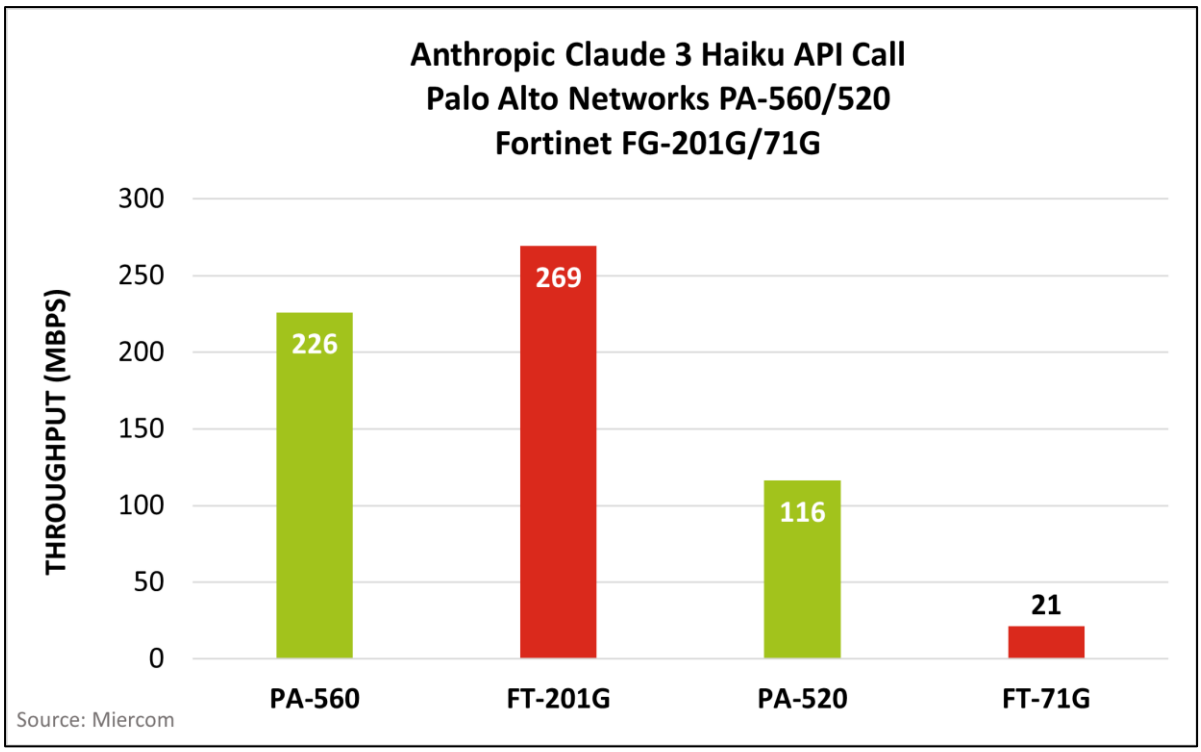
When handling OpenAI API traffic, Palo Alto Networks PA-560 recorded the highest throughput at 279 Mbps, closely followed by Fortinet FG-201G at 273 Mbps. The PA-520 reached 206 Mbps, providing nearly 10× the throughput of FG-71G, which was limited to 22 Mbps. This result shows that both Palo Alto Networks platforms delivered strong OpenAI API performance, while the lower tier Fortinet unit showed significant constraints.



For Gemini API calls using text prompts, throughput for Palo Alto Networks PA-560 and Fortinet FG-201G was comparable, at 260 Mbps and 265 Mbps, respectively. PA-520 achieved 186 Mbps, again far exceeding FG-71G, which reached only 22 Mbps. These results indicate that both vendors can support higher tier Gemini text workloads, while the Fortinet FG-71G provides only limited headroom.



In the more demanding Gemini image-prompt scenario, Palo Alto Networks PA-560 delivered the highest throughput at 2,767 Mbps, ahead of Fortinet FG-201G at 2,017 Mbps. At the lower tier, FG-71G achieved 777 Mbps, which exceeded the 601 Mbps measured for PA-520. Overall, the PA-560 provided the strongest performance for image-based AI workloads, while relative results at the mid-range tier varied by platform.



For Anthropic Claude 3 Haiku API traffic, Fortinet FG-201G again produced the highest throughput at 269 Mbps, with PA-560 close behind at 226 Mbps. PA-520 reached 116 Mbps, delivering more than five times the throughput of FG-71G at 21 Mbps. These results show that higher tier platforms from both vendors can support Claude 3 Haiku workloads, while the Fortinet FG-71G offers only minimal capacity.

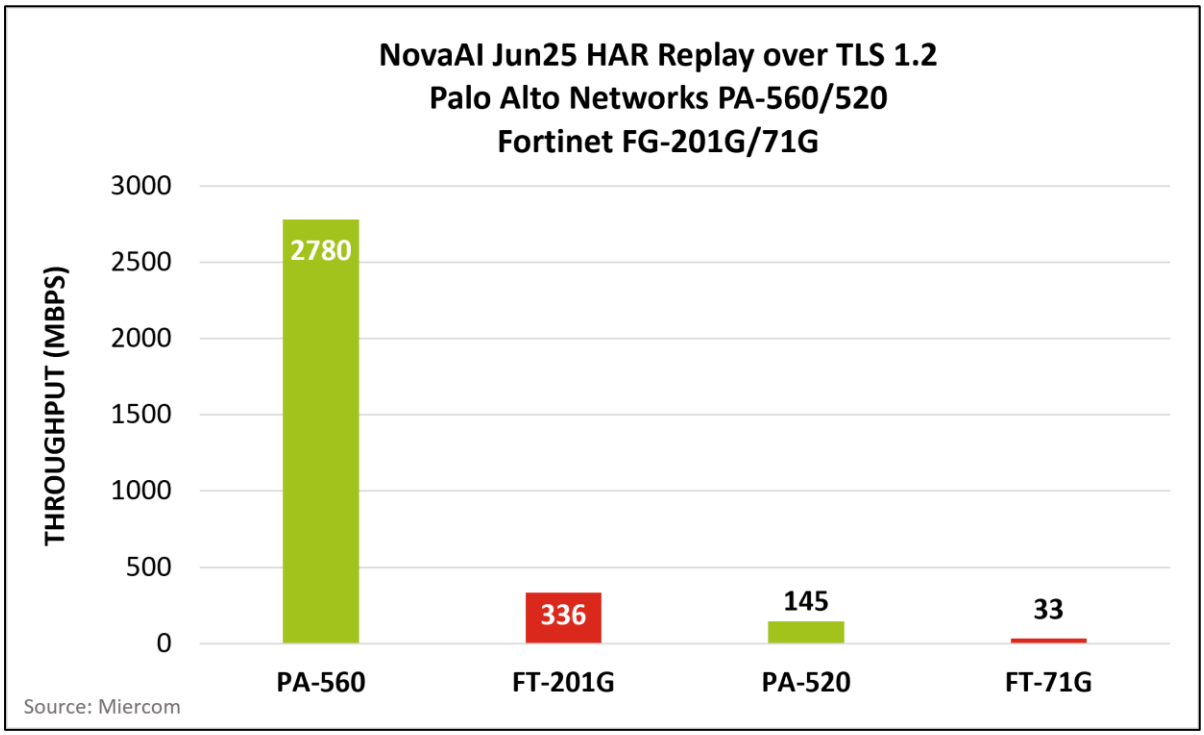
The Palo Alto Networks Advantage

Decisive AI Traffic Leadership Across All Tiers: Palo Alto Networks PA-560 and PA-520 demonstrated consistent, industry-leading throughput across all tested AI and LLM workflows (including OpenAI, Gemini, and Claude 3 Haiku), securing a critical capacity advantage against next-generation threats.

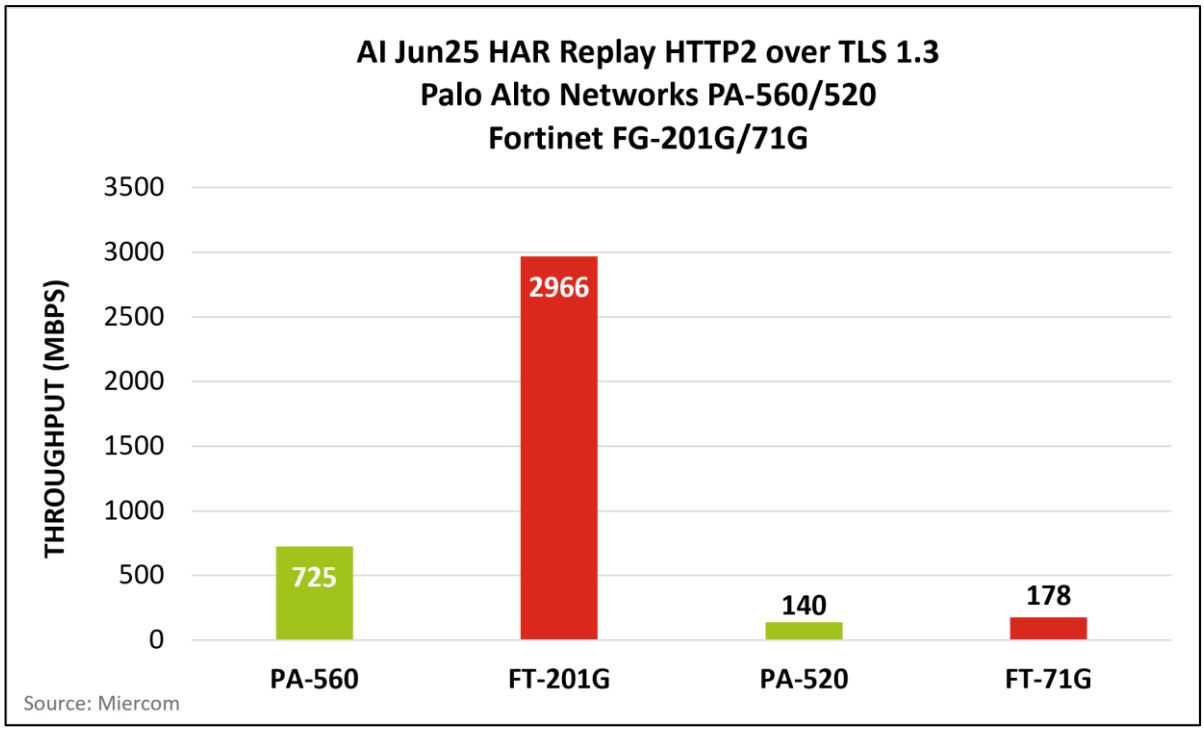
Critical Mid-Range Advantage: The PA-520 provided a stunning 5x to 10x higher throughput than the Fortinet FG-71G in every LLM text workflow, confirming that the Fortinet lower-tier platform offers minimal to no usable capacity for modern AI-centric business traffic. This makes the PA-520 the only viable mid-range platform for future AI adoption. At the top tier, the PA-560 consistently led or closely matched the FG-201G, delivering the highest overall throughput in the highly demanding Gemini image-prompt test (2,767 Mbps). While FG-201G led in some LLM and Claude scenarios, the performance gap between the two higher tier platforms was relatively small compared with the large disparity observed between PA-520 and FG-71G.

Taken together, these results show that Palo Alto Networks provides strong AI and API handling capabilities at both evaluated tiers, with a particularly pronounced advantage in the lower tier segment where Fortinet FG-71G exhibited severe limitations across all AI workloads.

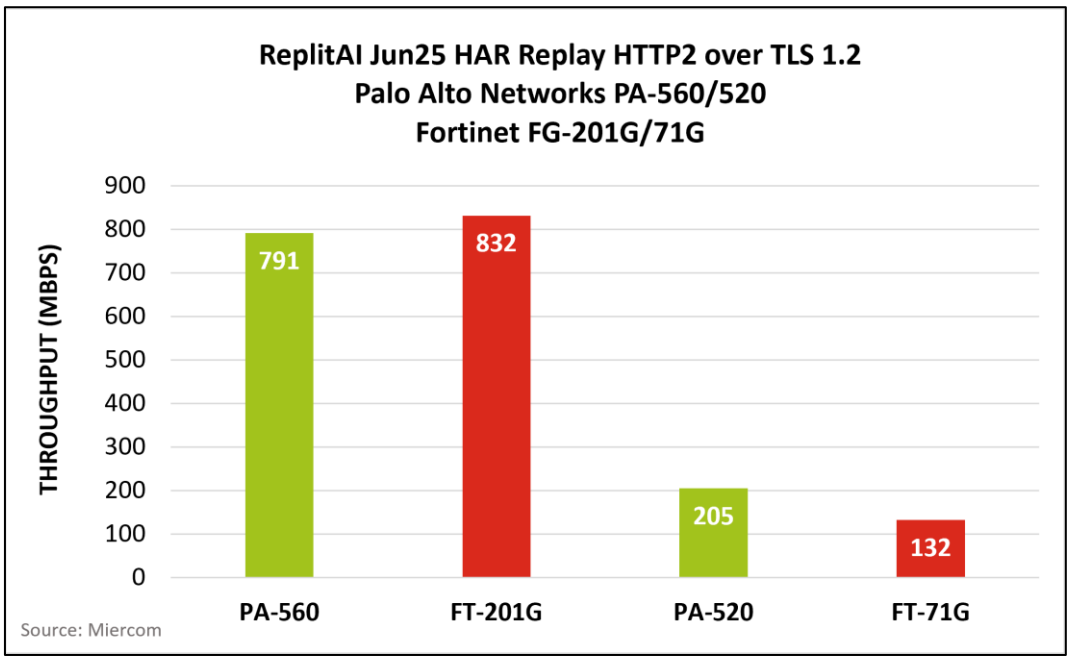
5.7.2 AI Replay's HTTP/HTTP2



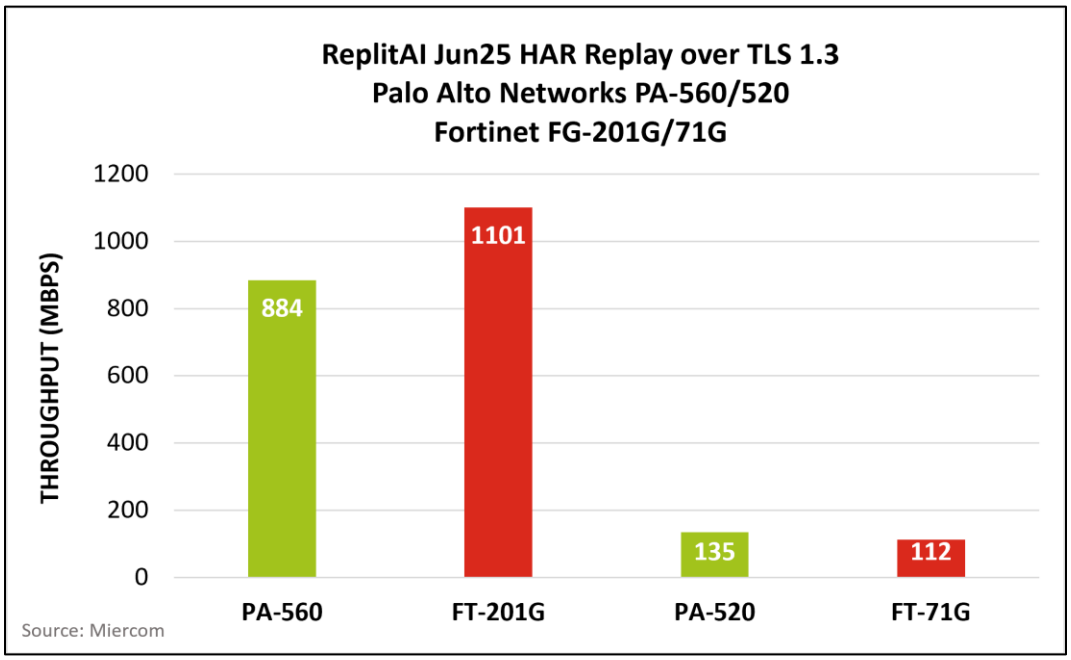
The PA-560 reached 2,780 Mbps, delivering over 8× higher throughput than the FG-201G at 336 Mbps. The PA-520 measured 145 Mbps, outperforming the FG-71G (33 Mbps) by more than 4×. These results reflect a significant performance lead for Palo Alto Networks under TLS 1.2 encrypted HAR replay.



The PA-560 achieved 725 Mbps, while the FG-201G reached 2,966 Mbps. For the mid-range platforms, the PA-520 recorded 140 Mbps, compared to 178 Mbps for the FG-71G. Results show Palo Alto Networks maintains competitive throughput under HTTP/2 over TLS 1.3, especially in the lower-capacity segment.



The PA-560 delivered 791 Mbps, performing slightly below the FG-201G at 832 Mbps. The PA-520 measured 205 Mbps, offering roughly 1.5× the throughput of the FG-71G (132 Mbps). Palo Alto Networks demonstrates stronger sustained performance in the lower-bandwidth tier under TLS 1.2.

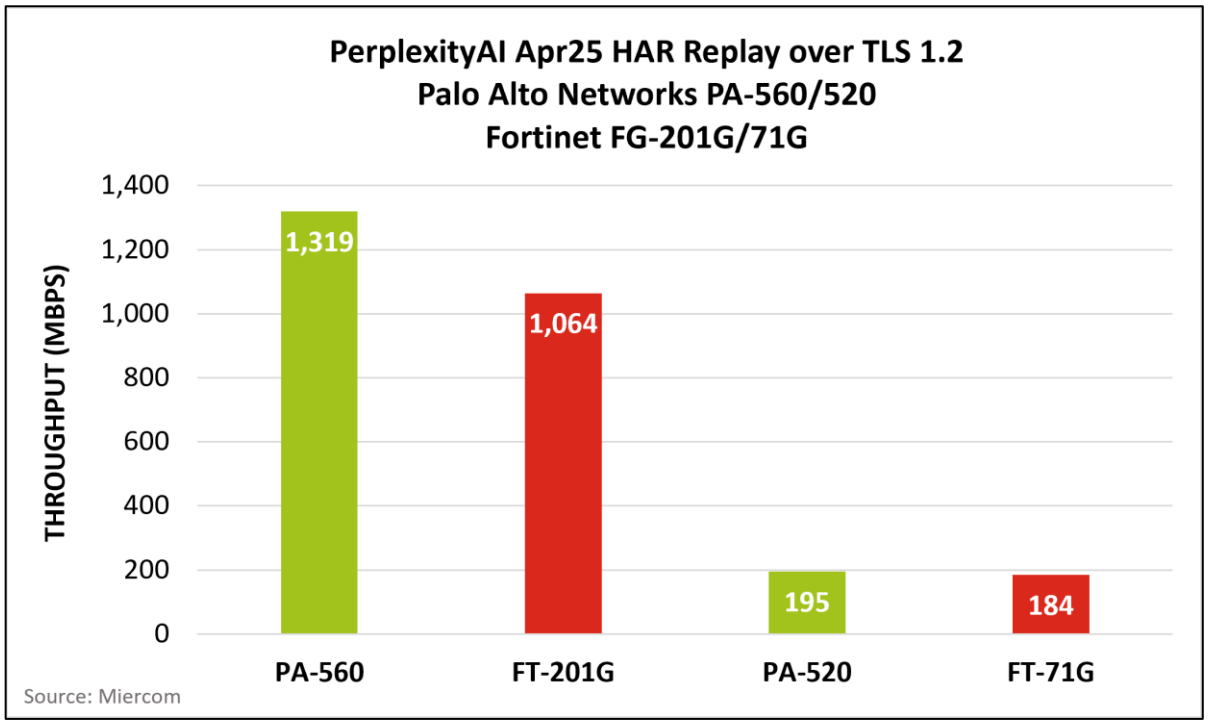


The PA-560 achieved 884 Mbps, while the FG-201G reached 1,101 Mbps. The PA-520 recorded 135 Mbps, exceeding the FG-71G's 112 Mbps by approximately 20 percent. Across TLS 1.3 encrypted replay, Palo Alto's PA-520 consistently outperforms the Fortinet 71G class.

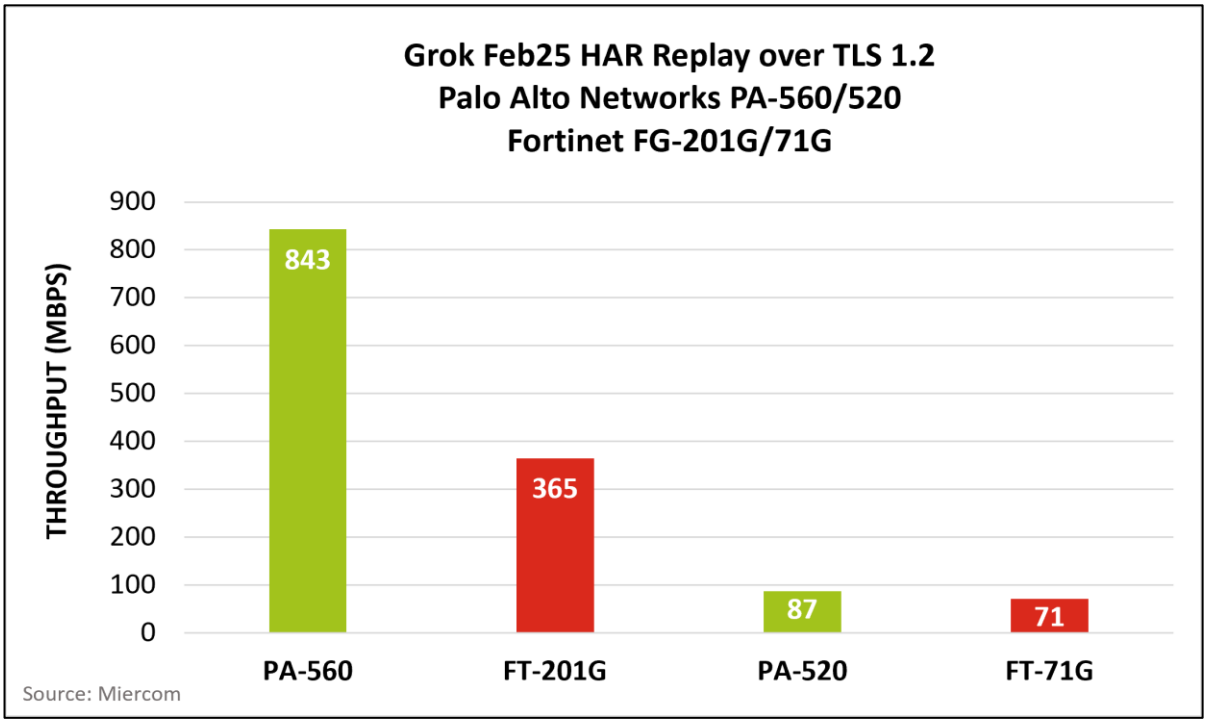
The Palo Alto Networks Advantage

Across all test scenarios, Palo Alto Networks shows consistent and repeatable performance strength in the mid-range class, with the PA-520 outperforming the Fortinet FG-71G in every workload ranging from 20% to over 4×. The PA-560 demonstrates significant leadership in certain encrypted TLS 1.2 workflows. Most notably the Nova AI test, where it surpasses the FG-201G by more than 8×. These combined results highlight Palo Alto Networks' ability to sustain high application replay throughput under varied encryption standards and AI-driven traffic patterns.

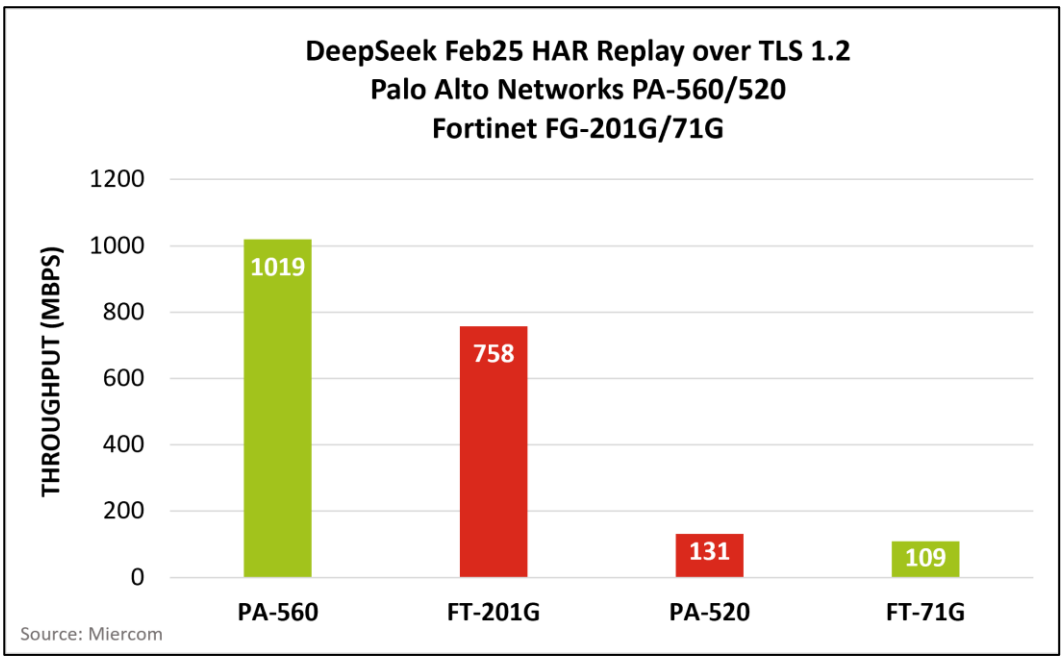
5.7.3 AI Replay's HTTP/HTTP2 (AI model set2)



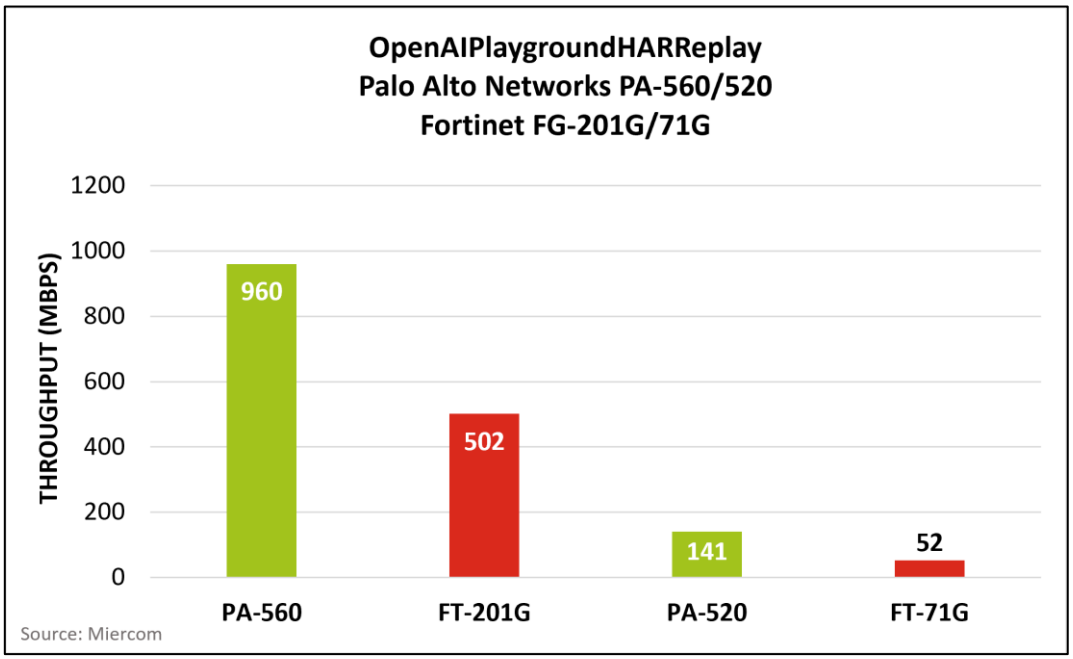
The PA-560 delivered 1,319 Mbps, which is 1.2× higher throughput than the FG-201G at 1,064 Mbps. The PA-520 achieved 195 Mbps and outperformed the FG-71G at 184 Mbps. Palo Alto Networks platforms maintained a measurable throughput advantage under the Perplexity AI replay workload.



The PA-560 reached 843 Mbps, providing 2.3× the throughput of the FG-201G at 365 Mbps. The PA-520 delivered 87 Mbps, which is 1.2× higher than the FG-71G result of 71 Mbps. These results show consistent performance gains for Palo Alto Networks devices on the Grok HAR replay test.



The PA-560 achieved 1,019 Mbps, outperforming the FG-201G at 758 Mbps by a factor of 1.3. The PA-520 recorded 131 Mbps, providing 1.2× the throughput of the FG-71G at 109 Mbps. Palo Alto Networks demonstrated stronger sustained performance across the DeepSeek traffic profile.



The PA-560 delivered 960 Mbps, which is 1.9× higher throughput than the FG-201G at 502 Mbps. The PA-520 reached 141 Mbps, outperforming the FG-71G at 52 Mbps by a factor of 2.7. Palo Alto Networks platforms showed clear performance advantages when processing the OpenAI Playground workload.

The Palo Alto Networks Advantage

Across all four HAR replay workloads, the PA-560 consistently delivered higher throughput than the FG-201G, with gains ranging from 1.2× to 2.3× depending on the traffic profile. The PA-520 also exceeded the performance of the FG-71G in every test, producing improvements from 1.2× up to 2.7×. These results show that both Palo Alto Networks platforms maintained stronger and more scalable TLS 1.2 inspection throughput across diverse AI-driven application traffic.

5.8 Memory Constraint Under AI Traffic Load: Architectural Stability Failure

Feature	FortiGate-201G (12 Cores)	PA-560 (10 Cores)
Observed Stability	Low	High
Behavior Under Load	Entered Conserve Mode due to memory exhaustion. *Note: Memory spike occurred while processing the AI traffic load through the IPS and Anti-virus engines)*	Maintained normal operation; did not enter Conserve Mode.
Trigger Point	Memory threshold breach, occurring before 100% CPU utilization. *Note: With 12 CPU cores.*	Successfully handled load through IPS engine without critical memory spike. *Note: With 10 CPU cores.*
Reproducibility	Consistently reproduced following the execution of 3-4 consecutive AI-related performance tests.	Stable across all AI-related performance tests.
Recovery Requirement	Required a manual administrative reboot to exit Conserve Mode.	No recovery action required.

The FortiGate-201G exhibits a performance limitation/design constraint in processing sustained, high-volume AI traffic that heavily engages its security processing engines (IPS/AV), leading to premature memory-induced Conserve Mode activation. This failure, triggered by memory exhaustion before CPU limits were reached, confirms that the architecture is fundamentally constrained by memory when inspecting the complex patterns of AI traffic.

In contrast, the PA-560 demonstrates superior stability and memory resource management under identical testing conditions, proving it is architecturally capable of sustaining modern, security-intensive AI workloads.

TCO and Performance Context

This architectural instability directly undermines the reported FortiGate value proposition:

- The Total Cost of Ownership (price per protected Mbps) of the PA-560 is 0.62× better than the FG-201G.
- The Performance (protected throughput) of the PA-560 is 1.86× better than the FG-201G. Ultimately, the FortiGate's lower stability and susceptibility to Conserve Mode under AI load means the "protected throughput" figures are unreliable, severely diminishing any perceived value compared to the consistently stable and high-performing PA-560.

This TCO analysis rigorously compared NGFW products based on the true cost of protected performance—the essential metric for securing modern, high-throughput enterprise environments dominated by AI and encrypted API traffic. 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 for each comparable pair.

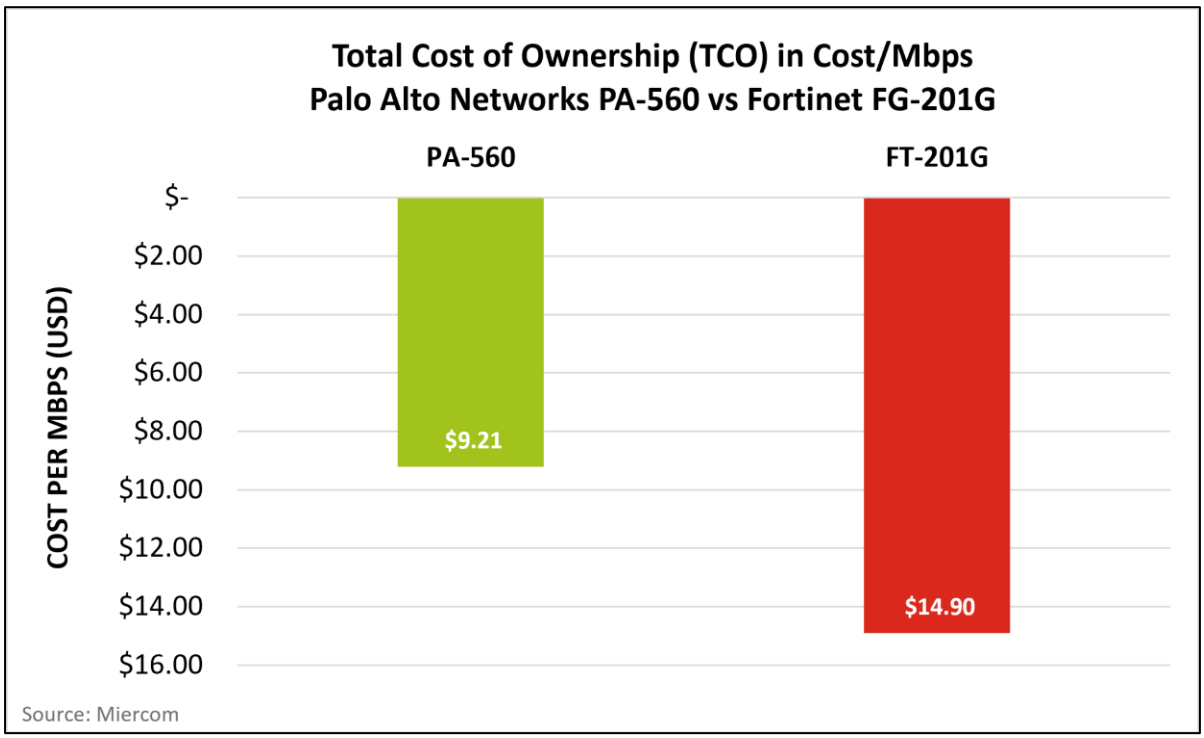
Palo Alto Networks PA-500 Series TCO Calculations					
Product	**Average Throughput (Mbps)**	**Total Cost (USD)**	**Hardware Cost (USD)**	**Subscription & Support Cost (USD)**	**Cost/Mbps**
PA-560	**3375**	**$31,090.08**	**$9,975**	**$19,950**	**$9.21**
PA-520	**685**	**$4,999.04**	**$1,675**	**$3324.04**	**$7.30**

Fortinet FortiGate TCO Calculations			
Product	**Average Throughput (Mbps)**	**Total Cost (USD) for 3 years Hardware + Subscription & Support Cost (USD)**	**Cost/Mbps**
FG-201G	**1813**	**$27,010**	**$14.90**
FG-71G	**273**	**$3,377.52**	**$12.38**

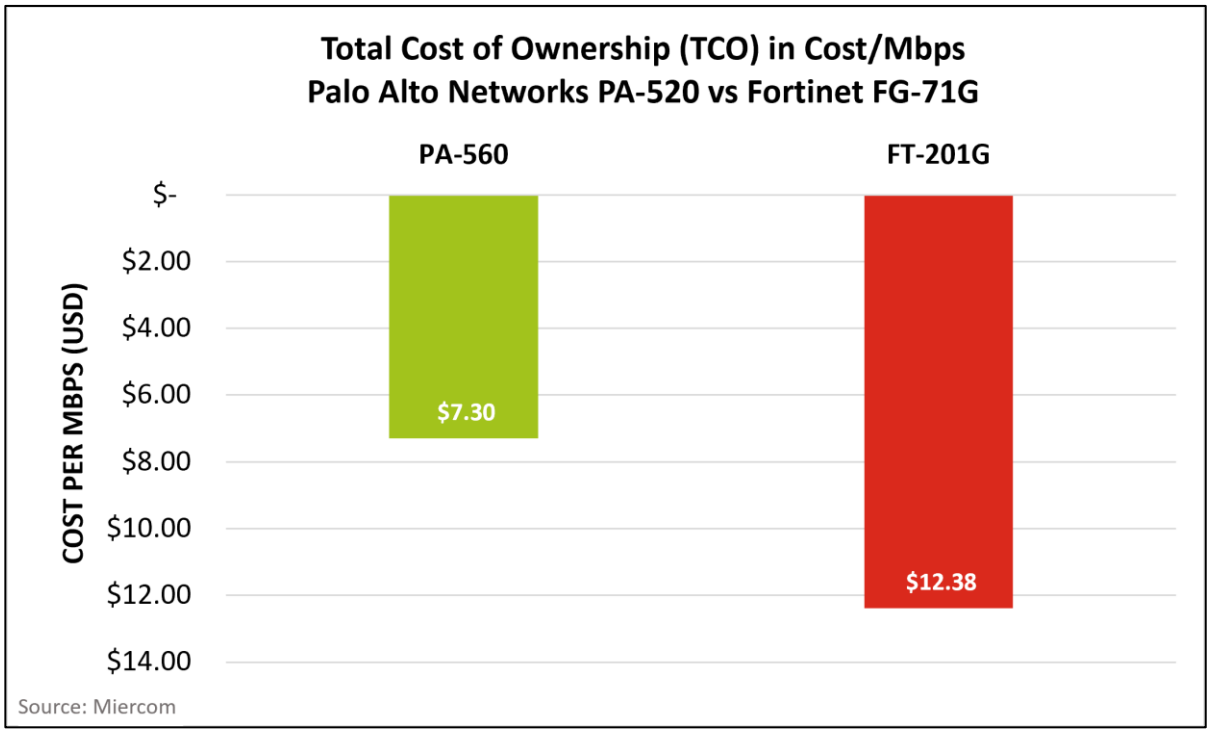
Note: Fortinet offers a bundle for their hardware + subscription and support.

Comparative Price and TCO Calculations: Palo Alto Networks vs Fortinet		
Product	**Price Difference (Hardware and Subscriptions)**	**TCO per Protected Mbps Difference**
PA-560 vs. FG-201G	***-13.1%***	***-61.8%***
PA-520 vs. FG-71G	***-32.4%***	***-69.6%***

Note: The total costs of acquisition are based on prices as of November 30th, 2025.



The PA-560 delivered a highly efficient Cost/Mbps of $9.21, representing a 38 percent lower cost compared to the Fortinet FG-201G at $14.90. This demonstrates that the PA-560 provides significantly more AI-ready protected throughput per dollar. This translates to a 1.6× improvement in TCO efficiency for the PA-560, securing substantially more AI-driven traffic per dollar under real-world, full-security conditions.



The mid-range PA-520 established market-leading value with a Cost/Mbps of just $7.30—a 41 percent lower cost than the FG-71G ($12.38). When considering the PA-520's 5× to 10× superior performance in critical LLM workloads, this TCO advantage makes it the most economical platform for distributed enterprises deploying AI applications This translates to a 1.7× better cost-efficiency for the PA-520, indicating significantly reduced total ownership cost for each protected Mbps delivered

7 Conclusion

DR251029C

The PA-500 series proved architecturally superior across performance, stability, and value. The FortiGate-201G exhibited a critical design flaw, entering a memory-induced Conserve Mode under sustained stress, specifically after Connections tests and during high-volume AI traffic, This failure point, which the PA-560 handled with superior stability, confirms a fundamental Fortinet limitation. Combining performance and cost, the PA-560 delivers 1.86×better protected throughput while offering a 0.62× better TCO (cost per protected Mbps) than the FG-201G. This decisive advantage is maintained in the mid-range, where the PA-520 provides protected throughput at approximately 41% lower cost per Mbps over its TCO than the FG-71G.

8 About Miercom

DR251029C

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.

9 Use of This Report

DR251029C

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% 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.

Miercom's Fair Test Policy allows for any vendor evaluated to challenge or retest these results in accordance with Miercom Terms of Use Agreement if there are any disagreements in our findings presented here.

Miercom did not acquire products for this review, nor has Miercom agreed to any vendor's End User License Agreement (EULA) or any other overly restrictive agreements that limit free press, product evaluations, editorial works, or publishing product reviews. We believe in providing accurate objective information to assist customers make informed purchasing decisions.

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:

- **Advanced Threat Prevention:** Analyze up to 673 million new sessions daily and proactively block 28.2 billion threats in real time including zero-day exploits, malware, command-and-control (C2) traffic, and evasive techniques to deliver cutting-edge security.
- **Anti-Virus Protection:** Provided through security profiles that inspect network traffic for known malware signatures, preventing infected files from reaching end-users. Enabled by creating or modifying an antivirus profile and attaching it to a security policy rule that allows traffic, the antivirus engine scans traffic using a stream-based approach. Its efficacy depends on up-to-date signature lists provided through licensing.
- **Anti-Spyware Protection:** Provided through configurable security profiles that inspect traffic for malicious activity. These profiles can be customized to define actions for specific threat signatures and DNS queries. Key features include signature policies, DNS security, and the option to enable advanced inline cloud analysis for real-time threat detection.
- **Advanced DNS Protection:** Real-time protection that instantly blocks sophisticated DNS request and response-based threats. It analyzes over 1.1 billion new domains daily and identifies up to 7.7 million newly malicious domains, preventing more than 2 billion threats inline. This powerful first line of defense identifies and stops threats at the DNS layer whether they originate from outside or within the network.
- **Application ID / Control:** Identifies and controls applications based on identity, not just port and protocol. It uses a combination of application signatures, protocol decoding, and heuristics to determine what application is running, even if it uses encryption or non-standard ports. This allows for granular security policies to enable, block, or inspect specific applications and their functions, providing greater visibility and control than traditional firewalls.
- **File Blocking:** Managed through **File Blocking profiles**, which are security profiles attached to security policy rules to control the upload and download of specific file types. These profiles can be configured to block, alert, or prompt users for actions on certain files, helping prevent malware and other threats by identifying and stopping malicious or unnecessary file transfers.
- **Wildfire Protection:** 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.
- **SSL Inspection (Profiles to be adjusted per test):** Decrypts encrypted traffic to inspect it for threats, which is accomplished by configuring **SSL Inbound Inspection** for traffic to internal servers or **SSL Forward Proxy** for outbound traffic. This involves importing the relevant certificates and private keys, creating a decryption profile to define settings and configuring a decryption policy rule to specify which traffic to decrypt. Security policy rules must be updated to allow the decrypted traffic to pass, and the configuration changes must be committed.

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-560	FG-201G
5.1 RAW TCP Throughput		
Raw TCP Throughput with 1 Bye Payload	1,520	355
5.2 Maximum HTTP 1.1 Bandwidth (Mbps) and Connections/sec (CPS) with 64/21/4.5K Payload		
64K Bandwidth	10,019	4,281
64K CPS	41,373	23,004
21K Bandwidth	6,399	2,151
21K CPS	47,132	24,510
4.5K Bandwidth	2,511	830
4.5K CPS	48,624	20,241
5.3 Real-World Single Application Performance (Mbps)		
SIP	3,536	2,177
MSSQL	5,954	1,951
FIX	2,582	1,166
RDP	2,080	1,430
SMBv2	8,589	5,416
FTP	9,878	9,880
5.4 TCP Maximum Capacity Concurrent TCP Sessions and Connections/sec (CPS)		
Maximum TCP Connections Per Second (CPS)	46,781	39,663
Maximum Concurrent TCP Sessions (CC)	538,336	251,293
5.5 Enterprise Traffic Mix (HTTP & HTTPS)		
Threat Throughput	8,775	2,032
5.6 Decryption Throughput Analysis		
TLS 1.2 Decryption Throughput ECDHE-AES-256-SHA-384-Single-64K-HTTP-GET-4K-key	2,682	1,645
TLS 1.2 Decryption Throughput ECDSA-AES-128-GCM-SHA256-P521Key-Single 64K HTTP GET	2,805	2,545
TLS 1.2 Decryption Throughput ECDHE-AES-128-SHA-256 Single 64K HTTP GET-2K Key	3,547	2,045
TLS 1.3 Decryption Throughput AES 256 SHA 3844K Key- Single HTTP GET Key	2,055	1,807
5.7 AI LLM		
5.7.1 LLM Text Workflows		
AI LLM over Generic HTTP	226	269
OpenAI API Call	279	273
Gemini API Call with Text Prompts	260	265
Gemini API Call with Image Prompts	2767	2017
Anthropic Claude3 Haiku API Call	234	304
5.7.2 AI Replay's HTTP/HTTP2		
Nova AI Jun25 HAR Replay over TLS 1.2	2780	336
AI Jun25 HAR Replay HTTP2 over TLS 1.3	725	2966
Replit AI Jun25 HAR Replay HTTP2 over TLS 1.2	791	832
Replit AI Jun25 HAR Replay over TLS 1.3	884	1101
5.7.3 AI Replay's HTTP/HTTP2 (AI model set2)		
Perplexity AI Apr25 HAR Replay over TLS 1.2	1,319	1,064
Grok Feb25 HAR Replay over TLS 1.2	843	365
DeepSeek Feb25 HAR Replay over TLS 1.2	1019	758
OpenAI Playground HAR Replay	960	502

Test	PA-520	FG-71G
5.1 RAW TCP Throughput		
Raw TCP Throughput with 1 Bye Payload	377	75
5.2 Maximum HTTP 1.1 Bandwidth (Mbps) and Connections/sec (CPS) with 64/21/4.5K Payload		
64K Bandwidth	1,842	652
64K CPS	11,731	6,086
21K Bandwidth	1,439	371
21K CPS	12,525	8,335
4.5K Bandwidth	552	241
4.5K CPS	13,220	6,750
5.3 Real-World Single Application Performance (Mbps)		
SIP	1,015	495
MSSQL	551	600
FIX	723	248
RDP	627	153
SMBv2	1,727	952
FTP	2,003	756
5.4 TCP Maximum Capacity Concurrent TCP Sessions and Connections/sec (CPS)		
Maximum TCP Connections Per Second (CPS)	11,458	8,520
Maximum Concurrent TCP Sessions (CC)	103,559	67,413
5.5 Enterprise Traffic Mix (HTTP & HTTPS)		
Threat Throughput	1,714	342
5.6 Decryption Throughput Analysis		
TLS 1.2 Decryption Throughput ECDHE-AES-256-SHA-384-Single-64K-HTTP-GET-4K-key	492	193
TLS 1.2 Decryption Throughput ECDSA-AES-128-GCM-SHA256-P521Key-Single 64K HTTP GET	976	337
TLS 1.2 Decryption Throughput ECDHE-AES-128-SHA-256 Single 64K HTTP GET-2K Key	517	298
TLS 1.3 Decryption Throughput AES 256 SHA 3844K Key- Single HTTP GET Key	251	50
TLS 1.2 Decryption Throughput ECDHE-RSA-AES256-GCM-SHA384-64K HTTP GET-2K Key	732	490
5.7 AI LLM		
5.7.1 LLM Text Workflows		
AI LLM over Generic HTTP	116	21
OpenAI API Call	206	22
Gemini API Call with Text Prompts	186	22
Gemini API Call with Image Prompts	601	777
Anthropic Claude3 Haiku API Call	208	39
5.7.2 AI Replay's HTTP/HTTP2		
Nova AI Jun25 HAR Replay over TLS 1.2	145	33
AI Jun25 HAR Replay HTTP2 over TLS 1.3	140	178
Replit AI Jun25 HAR Replay HTTP2 over TLS 1.2	205	132
Replit AI Jun25 HAR Replay over TLS 1.3	135	112
5.7.3 AI Replay's HTTP/HTTP2 (AI model set2)		
Perplexity AI Apr25 HAR Replay over TLS 1.2	195	184
Grok Feb25 HAR Replay over TLS 1.2	87	71
DeepSeek Feb25 HAR Replay over TLS 1.2	131	109
OpenAI Playground HAR Replay	141	52