FORTINET

Five Advantages of Fortinet Data Center Firewalls

Table of Contents

Executive Summary

Digital transformation has profoundly impacted how businesses operate, enabling companies to leverage advanced technologies to improve efficiency, productivity, and innovation. This shift from traditional, manual processes to more automated, data-driven approaches has led to better customer experiences and increased profitability. It has also had an intense impact on IT networks.

With the vast amount of data now traversing the network through physical, virtual, and cloud IT infrastructures, the central importance of the data center in today's distributed networks cannot be ignored. And because of this, securing today's complex data center environments must be a top priority.

Fortinet's comprehensive portfolio of data center cybersecurity solutions, including FortiGate Next-Generation Firewalls (NGFWs), enable organizations to build the dynamic, hybrid environments organizations need without compromising on security or performance.

Here are the top five reasons to choose Fortinet for your next data center firewall solution.

Highest Performance

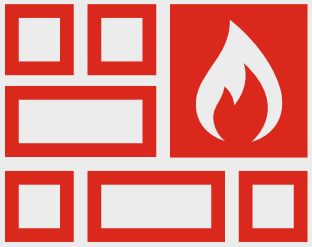
Fortinet is the only vendor to leverage custom ASIC technology to support the high-performance and resource-intensive requirements of today's data centers. We are also the only vendor to offer scalable 400G I/O ports with integrated routing for ultra-low, single-digit microsecond latency. This emphasis on performance delivers critical advantages: By processing and analyzing data more quickly, FortiGate firewalls identify and block potential threats in real time. Encrypted data and streaming video can be inspected without impacting network performance. And faster network speeds ensure that applications can be optimized for better productivity and a consistent user experience.

Fortinet's data center firewalls deliver five times the performance of the industry average, eight times the industry average for SSL inspection throughput,[1] and three times the industry average for firewall throughput.[2,3]

Advanced Threat Protection

The FortiGuard AI-Powered Security Suite leverages artificial intelligence (AI) and machine learning (ML) to provide advanced threat protection across its comprehensive security portfolio. It continuously assesses risks and automatically responds to and counters known and unknown threats across all threat vectors, including network, endpoint, cloud, and application security. And because FortiGate data center firewalls are also natively part of the Fortinet Security Fabric, they are fully integrated into the extended fabric, ensuring coordinated detection and enforcement across your entire attack surface. This unique framework approach can rapidly adjust its security posture to detect and respond to newly discovered attacks, regardless of where in your network they occur.

- **Enhanced threat detection:** ML algorithms detect advanced threats that traditional security solutions may miss to identify and respond to threats more quickly and effectively.
- **Proactive threat response:** AI-powered automation responds to threats in real time to contain and remediate threats before they can cause significant damage.
- **Improved accuracy:** AI and ML improve the accuracy of threat detection, reducing false positives and providing more accurate threat intelligence.
- **Reduced security management overhead:** Consolidating security functions reduces complexity while lowering costs and improving efficiency.
- **Scalability:** High scalability allows businesses to add new security functions and increase capacity without additional management overhead.
- **Comprehensive coverage:** Comprehensive security covers all threat vectors, including data center, campus, branch endpoint, cloud, and application security.
- **Advanced functionality:** The only vendor to include SD-WAN, ZTNA, inline sandboxing, and SOC-as-a-Service in their firewall platform.



Fortinet's unique converged approach also enables our firewalls to be seamlessly incorporated into a hybrid mesh firewall architecture that "enables security policy controls to be defined and workloads connected on any network in on-premises-first organizations."[4]

Unified FortiOS

FortiOS is the unified operating system (OS) that runs the broad portfolio of technologies that are part of the Fortinet Security Fabric. This includes our hybrid mesh firewall (HMF), a unified security platform for deploying consistent management and analytics across your entire distributed network. This unified OS approach delivers comprehensive visibility and protection against security threats, simplifies operations, ensures compliance, and reduces complexity to increase operational efficiency. It also authenticates and grants explicit access to applications and data center resources, allowing organizations to consolidate crucial security and networking capabilities.

- **Enhanced security:** Consistently enforces policies across all security devices to protect against advanced threats, including ransomware malware, viruses, and other cyberattacks.
- **Simplified management:** Its unified management console reduces the time and resources required to manage security, allowing IT teams can focus on other priorities.
- **Improved visibility:** Broad deployment delivers deep visibility into network activity and security events so administrators can identify and respond to security threats quickly and effectively.
- **Increased scalability:** High scalability allows businesses to extend capacity without having to manage multiple operating systems to reduce complexity and enable faster growth.
- **Better performance:** FortiOS is optimized for performance, providing the industry's fastest and most reliable security across all devices.

According to IDC, Fortinet holds the No. 1 position for units shipped at more than 8.4 million for a market share of 48%.[5]

Enhanced Sustainability

Fortinet data center firewalls are the most energy-efficient in the industry, helping organizations save on energy consumption and reduce their carbon footprints. Our FortiGate data center firewalls are also designed to operate with high efficiency and low power consumption, reducing the total cost of ownership. They consume 66% less power than rival solutions,[6] use 83% fewer watts per Gbps of throughput,[7] and are 6.5X more energy-efficient (BTU/h per Gbps) than competitive solutions.[8]

Aggressive ROI

Fortinet data center firewalls, combined with our AI/ML security services, provide the best price-performance ratio in the industry, delivering an aggressive ROI. Current FortiGate customers have experienced the following:

- 50% lower cost for a global technology service provider[9]
- 500 hours saved by the IT team at a top U.S. school district[10]
- $5M saved through IT cybersecurity consolidation by a leading U.S. university[11]
- $800K saved by a North American bottler[12]

- **Recognized as a Leader in the Gartner® Magic Quadrant™ for Network Firewalls 13 times[13]**
- **Positioned highest for Ability to Execute in the 2022 Gartner® Magic Quadrant™ for Firewalls[14]**
- **Received the highest scores for the Enterprise Data Center Use Case in the Gartner® Critical Capabilities for Network Firewalls four times in a row[15]**
- **Recognized as a leader in the Forrester Wave™: Enterprise Firewalls, Q4 2022 report[16] (Oct 2022)**

Summary

Fortinet data center firewalls offer several critical advantages, including better performance, advanced threat protection, unified FortiOS, broad security coverage, energy efficiency, and a strong ROI. These advantages make Fortinet data center firewalls an excellent choice for organizations seeking high-performance network protection with an impressive ROI.

[1] The average of SSL Inspection throughput for all Fortinet firewall models for the data center versus an aggregate average of published SSL Inspection throughput data of similar competitive models.

[2] The average of IPv4 firewall throughput for all Fortinet firewall models for the data center versus an aggregate average of published IPv4 firewall throughput of similar competitive models.

[3] Fortinet, "A comprehensive data center cybersecurity solution," March, 2023.

[4] Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur, Adam Hils, Tom Lintemuth, 19 December 2022.

[5] Nancy Liu, Fortinet Continues to Invest in Custom Chips to Power Security Offerings, SDX Central, 9 February 2023.

[6] Based on new models of the 2022 FortiGate F series (compared to equivalent models from the previous generation).

[7] FG-1000F versus competitors.

[8] Fortinet Press Release, "Fortinet's Latest Next-Gen Firewall Helps Customers Achieve Sustainability Goals by Consuming 80% Less Power Than Rivals," 2 November, 2022.

[9] Synacor case study.

[10] School District of Philadelphia case study.

[11] University of South Carolina case study.

[12] Available upon request with a signed NDA.

[13] Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur, Adam Hils, Tom Lintemuth, 19 December 2022.

[14] Ibid.

[15] Gartner, Critical Capabilities for Network Firewalls, Adam Hils, Rajpreet Kaur, Thomas Lintemuth, 17 May 2023.

[16] Forrester, Forrester Wave™: Enterprise Firewalls, Q4 2022 report, Oct 2022.

FORTINET

www.fortinet.com

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

September 22, 2023 5:56 PM

2151789-A-0-EN