# Data Center Firewall Toolkit

FORTINET

# Table of Contents

CHECKLIST

# Top 5 Reasons to Choose a Fortinet Data Center Firewall

**Digital transformation enables organizations to leverage technology for increased efficiency, productivity, innovation, and profitability, leading to better customer experiences. However, this shift to data-driven processes has placed a significant strain on IT networks, making high-performance data center security crucial for business success. Fortinet's comprehensive portfolio of FortiGate Next-Generation Firewalls (NGFWs) and FortiGuard AI-Powered Security Services deliver:**

## Unmatched Performance

Fortinet is the only firewall vendor that employs patented ASIC technologies rather than general-purpose processors. This industry-exclusive approach increases performance and throughput, enabling faster and more accurate detection, even when threats are hidden in encrypted traffic and streaming video. There is no need to sacrifice security for performance with FortiGate.

## Proven Protection

FortiGuard AI-Powered Security Services integrate with FortiGates and leverage AI and ML to provide market-leading security capabilities that protect application content, web traffic, devices, and users. These protections continuously assess risks and automatically respond to and counter known and unknown threats detected anywhere across the distributed network. Coordinated and consistent real-time services defend against even the very latest, AI-driven, and evasive attacks.

## Unification

FortiGate is the cornerstone of the Fortinet Security Fabric platform. A single operating system, FortiOS, unifies security, networking, and management. It supports all form factors and can be deployed at all edges to consistently defend and coordinate hybrid environments. This unique approach enables organizations to consolidate critical security and networking capabilities, closing security gaps, speeding threat response, and ensuring direct access to application and data center resources.

## Sustainability

Fortinet's low-power, environmentally friendly cybersecurity network solutions help enterprises save on energy consumption, heat dissipation, and space, reducing overall energy spend. Powered by purpose-built security processing units (SPUs), Fortinet firewalls enable energy efficiency that lowers operational costs while promoting environmental responsibility. Fortinet solutions require less power to generate 1G of firewall throughput than comparable solutions.

## Better ROI

Fortinet data center firewalls combine high performance with low power consumption and real-time AI/ML security services to deliver a better return on investment:

- 99.9% network availability[1]
- 60% boost in IT team efficiency[2]
- 50% less time spent on firewall management[3]

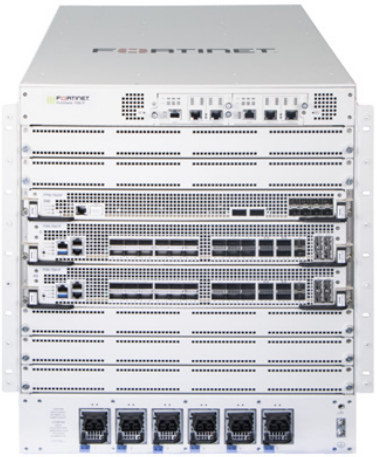
## Conclusion

FortiGate NGFWs are the best choice for today's data centers for many reasons. Key differentiators include proprietary ASICs that accelerate security and networking performance to effectively secure the growing volume of data-rich traffic. And, thanks to industry-leading FortiGuard AI-Powered Security Services, cyberattacks and security risks are mitigated with consistent, real-time protection and responses against even the newest and most sophisticated threats.

INDUSTRY INSIGHTS

# Boost Your Data Center's Performance and Security with the FortiGate 7000F Series

## Data Center Firewalls Are a Critical Element of the Hybrid Network



To keep up with rapid change and the expanding attack surface, caused in part by distributed workforces, today's organizations need agile hybrid network architectures. While this fusion of physical, virtual, and cloud infrastructure reshapes data center roles, it doesn't eliminate their importance or the requirement for robust security. The data center is still key for housing applications and data that is not located in the cloud. As such, data center firewalls remain critical for protecting against evolving threats across complex, hybrid environments, ensuring secure, high-volume traffic flow between data centers, cloud, branches, and remote users.

## FortiGate: Far Better Than the Industry Standard

The FortiGate 7000F series delivers unparalleled value as an all-in-one cybersecurity solution that integrates high-performance networking and security. Designed to safeguard mission-critical data across hybrid IT infrastructures, it provides:

- 5x more next-generation firewall (NGFW) throughput
- 2x improved threat protection
- 2x IPsec VPN throughput
- 73% more energy-efficiency per Gbps

Consolidating security services into a single, easy-to-manage platform with AI-powered protection and automation reduces operational complexity and improves compliance. The FortiGate 7000F series eco-friendly design helps enterprises lower energy costs while maintaining top-tier security. As the only NGFW offering built-in SD-WAN, universal ZTNA, inline sandboxing, and SOC-as-a-Service, the FortiGate 7000F series optimizes performance, scalability, and ROI.

| Specification | FortiGate 7080F | Security Compute Rating | Industry Average | Palo Alto Networks PA-5450 | Check Point QLS 800 | Cisco Firepower 9300 | Juniper Networks SRX 5800 |
|---|---|---|---|---|---|---|---|
| **Firewall (Gbps)** | 1190 | 2.9x | 410 | 200 | 205 | 235 | 1000 |
| **NGFW (Gbps)** | 330 | 5.3x | 62.5 | - | 96 | 29 | - |
| **IPsec VPN (Gbps)** | 370 | 3.4x | 110 | 87 | 49 | 74 | 230 |
| **Threat protection (Gbps)** | 312 | 3.4x | 92.5 | 152.5 | 33 | - | - |
| **SSL inspection (Gbps)** | 320 | 11.4x | 28 | - | - | 28 | - |
| **Concurrent sessions** | 600 million | 3.6x | ~166 million | 100 million | 32 million | 195 million | 338 million |
| **Watts per Gbps threat protection** | 23.4 | 2.5x | 58.5 | 23 | 93.9 | - | - |

## Eliminate Point Products and Reduce Complexity

Building on Fortinet's proven high-performance security, the FortiGate 7000F series eliminates point products by consolidating security functions to reduce complexity and deliver industry-leading ROI. With 1.2 Tbps firewall throughput and 312 Gbps threat protection, the FortiGate 7000F series significantly outperforms competitors while consuming less power. The modular design, featuring an energy-efficient chassis, Fortinet processor modules, and 400 GE ports, simplifies scaling and ensures businesses can adapt to evolving network demands without operational downtime. Fortinet remains the sole vendor offering 400 GE ports, providing a significant advantage.

## Get the ASIC Advantage

Fortinet's proprietary ASIC architecture delivers unmatched security performance and efficiency, ensuring your organization can scale without compromising speed or protection. By providing faster threat prevention with lower latency, it enables seamless user experiences and keeps critical applications running smoothly. Its energy-efficient design reduces power consumption and cooling costs, driving significant cost savings while supporting sustainability goals.

With higher performance at a lower total cost of ownership, FortiGate lets your organization optimize resources, reduce operational complexity, and future-proof its network infrastructure. Fortinet's ASIC-powered security ensures maximum protection, minimal delays, and a stronger return on investment, so you can focus on business growth with confidence.

Our NP7 network processor delivers trail-blazing VXLAN hardware acceleration and IPsec elephant flows. The NP7 is designed to accelerate essential network functions, such as IPv4, IPv6, multicast, GRE, and IPsec decryption, among others. And the FortiGate 7000F series supports 4.5 million connections per second session setup speeds for firewall and NAT sessions, supplying hyperscale security for hyperscale data centers.

## Accelerate Security Functions

The FortiGate 7000F series also addresses the need to find and mitigate risk as quickly as possible. Our CP9 content processor acts as a co-processor to the main CPU to offload resource-intensive processing and drive content inspection to accelerate security functions. Additionally, the CP9 performs fast inspection of real-time traffic for application identification, all without compromising user experience. It enables full network visibility, thus eliminating blind spots.

The parallel path processing architecture embodied with our latest NP7 and CP9 security processors offers unmatched L4–L7 performance. These capabilities build on the industry-leading security and threat detection included in all of the Fortinet NGFW offerings:

- The FortiOS operating system is the foundation of the Fortinet Security Fabric, the industry's highest-performing cybersecurity mesh platform that delivers coordinated detection and enforcement across the entire attack surface. FortiOS provides centralized, unified management and visibility across the network.
- FortiGuard AI-Powered Security Services, developed by FortiGuard Labs (the Fortinet elite cybersecurity research organization), counters threats in real time with machine-learning-powered, coordinated protection.
- Intrusion prevention provides the most up-to-date defenses against stealthy network-level threats to protect organizations from thousands of IPS signatures covering known vulnerabilities and exploits.
- The application control service quickly creates policies to allow, deny, or restrict access to applications or entire categories of applications to keep malicious, risky, and unwanted applications out of your network through control points like the data center.

## FortiGates: The Ideal Hybrid Mesh Firewalls

As businesses increasingly turn to hybrid environments to address the rise in cloud-based applications and remote workforces, it's critical for NGFWs to work in conjunction with firewalls deployed across the network, including in the cloud.

Hybrid mesh firewall (HMF) is an emerging term for a unified security platform that provides coordinated protection to multiple areas of enterprise IT, including corporate sites such as branches, campuses, and data centers; public and private clouds; and remote workers.

Because FortiGate and all other Fortinet firewall solutions were and continue to be built on FortiOS, we have delivered on the HMF concept for years. Using Fortinet solutions empowers IT teams with centralized, unified management and an open ecosystem that enables consistent security policies across all firewall deployments.

To learn more about the FortiGate 7000F series and our associated services for the data center, visit the Fortinet NGFW webpage.

CHECKLIST

# Top 6 Recommendations to Improve User Productivity with a Hybrid Architecture

The speed of business is accelerating the data center's journey toward digital transformation, requiring new hybrid network architectures that combine on-premises data centers with multiple public and private cloud deployments to form a hybrid mesh firewall (HMF) environment. However, to meet the needs of organizations expanding their digital transformation, the underlying enabling technologies must be more reliable and energy-efficient. They must also deliver consistent security across the hybrid architecture to defend against threats.

On-premises and virtual data centers are vital in today's ever-evolving network. In this new model, security is essential to protect resources and assets and to enable the network to accelerate and adapt without introducing unknown risks that can jeopardize the enterprise.

## 6 Things Organizations Need to do to Position Themselves for Success

### ☑ Invest in a Flexible Next-Generation Firewall

Organizations need to invest in a next-generation firewall that includes technologies like SD-WAN, universal ZTNA, inline sandbox, and SOC-as-a-Service. These technologies improve WAN connectivity by providing better user experience with direct internet access, while LAN and WLAN provide faster access to local devices and users.

### ☑ Deploy Unified Networking and Security

Security can't be an afterthought. When security solutions are not well-integrated with each other or the underlying network, security risks and gaps arise as the attack surface expands and adapts. These blind spots are vulnerable to sophisticated multi-step attacks and are partly responsible for the dramatic rise in successful ransomware attacks. Hence, it is important to look for a unified security framework to deliver automated and reactive security that spans the HMF architecture for all firewall deployments to cover the entire attack surface. Organizations must also converge their security with networking to protect digital acceleration efforts.

### ☑ Adopt a Secure-Networking Strategy

With new network edges being created on-premises and in the cloud, it is critical that the unified convergence of networking and security be available everywhere, combined with ZTNA to enable explicit access for applications and continuous verification of users and devices. This convergence is the heart of a secure networking strategy. Also, flexibility in providing this convergence is key in securing digital acceleration for hybrid deployments.

### ☑ Speed Operations with Centralized and Automated Management

The exponential growth of network edges, cloud platforms, and tools can significantly increase operational complexity. Furthermore, poor visibility and analytics gaps in the network along with tasks performed manually degrade the end-to-end digital experience.

These issues increase the time to configure, manage, and troubleshoot. They also add to operation costs and errors that can cause network outages and reduce flexibility. A hybrid mesh firewall architecture provides centralized and automated management to unify and deliver consistent security policies and network services across the organization. Removing manual configuration eliminates a major cause of downtime and security breaches.

## Increase Visibility with End-to-End Digital Experience Monitoring

Traditional network performance monitoring, IT infrastructure monitoring, and application performance monitoring provide network operations center (NOC) teams with limited visibility. These types of monitoring don't provide the performance insights into critical business applications that organizations need. They also severely hinder the visibility that frontline NOC and help desk teams need to resolve issues.

A modern digital experience monitoring (DEM) platform is required to give your NOC team superior visibility. It allows for the observation of any application, starting from the end-user, across any network, and to the infrastructure the application is hosted on. It can enrich incident management and supply holistic remediation of performance issues to resolve problems before users are impacted.

## Consolidate and Simplify Operations to Provide Instant ROI

Organizations adopting HMFs with unified management and integrated security achieve better ROI than those using point products with limited security. Secure networking also improves employee productivity with better user experience and simplified operations.

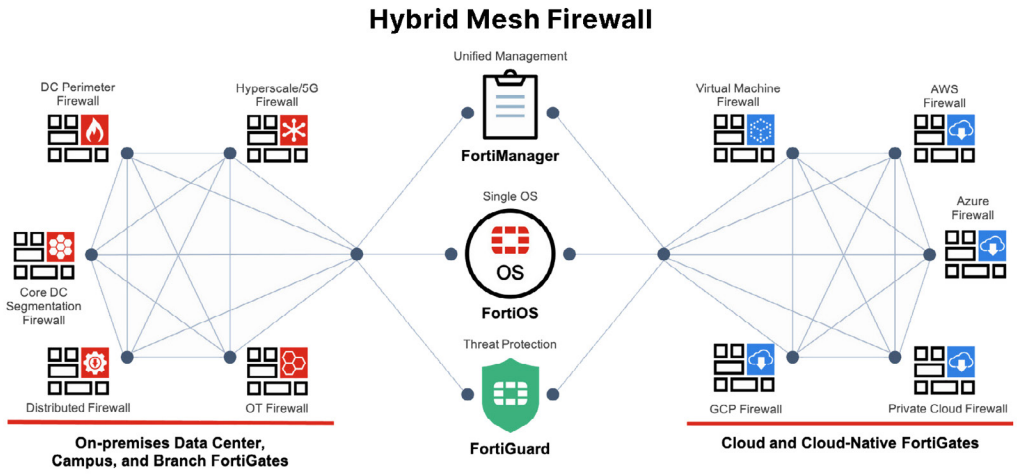



Figure 1: The Fortinet Hybrid Mesh Firewall solution

## Conclusion

Many organizations still use a traditional architecture to connect offices to the data center for application access. However, with users working from anywhere and applications distributed across multi-cloud and SaaS environments, this legacy network design is an obstacle for digital acceleration and creates user experience challenges. Organizations that want to have better user productivity and secure network edges need to invest in a modern hybrid network architecture.

Fortinet is the only vendor in the industry to offer an NGFW that includes SD-WAN, universal ZTNA, inline sandbox, and SOC-as-a-Service that can protect any edge at any scale. Offering the best convergence of networking and security, Fortinet empowers organizations to adopt modern networking technologies essential for digital acceleration. Learn more about Fortinet Secure Networking.

CASE STUDY

# Insurance Broker USI Ensures WAN Security Plus Higher Performance, Less Downtime, and Streamlined Management

As one of the world's largest insurance brokerage and consulting firms, USI Insurance Services works with a wide array of businesses and individuals, specializing in delivering property and casualty insurance, employee benefits, personal risk, and program and retirement solutions.

USI has been on a dramatic growth trajectory ever since its founding in 1994. In less than 30 years, it has ballooned from 40 employees generating $6.5 million in annual revenue to more than 9,000 associates and more than $2 billion in revenue. "We have experienced hypergrowth," explains Senior Network Engineer Joe Mogelinski. "I have been with USI for about six years, and the company has doubled since I started."

This hypergrowth has resulted in a corporate wide area network (WAN) that spans the United States. Mogelinski's team of three network engineers is responsible for network and security management, with assistance from about 25 regional IT operations professionals. A group of analysts set security policy and monitor security events, "but they are not the ones deploying the technology," Mogelinski says. "For the three of us to manage networking and security in 182 offices from coast to coast, it is imperative that we minimize complexity."

## Eye-Opening Deployment of Data Center Firewalls

As an insurance brokerage and consulting firm, USI handles highly sensitive information, most of which resides in the company's two data centers. And until recently, all communication to and from the 182 offices was backhauled to the data centers. Thus, Mogelinski and his team's top cybersecurity priority has long been securing the network edge.

That is why, when the headend firewalls in the data centers needed a refresh a couple of years ago, the team evaluated multiple options to be sure they were using the best possible technology. USI's security analysts had relied on the FortiSIEM security information and event management solution for several years. Still, most of the company's networking and security infrastructure—including the data center firewalls—was standardized on another industry leader. USI considered FortiGate NGFWs, the legacy edge security solution, and another competitor.

"We had a bake-off among the three heavy hitters from the Network Firewall Analyst Report," Mogelinski says. "We weighed all the pros and cons. A huge negative for the legacy firewalls was that they were very difficult to manage and maintain. As a result of our analysis, we ended up replacing our legacy firewalls with FortiGates, and we introduced FortiManager and FortiAnalyzer to manage them. Once we deployed the Fortinet solutions, we fell in love." USI engaged FortiCare Professional Services to help with the implementation and to bring Mogelinski and his team up to speed. "We quickly got good at managing them," he says. "Right away, we were very happy with the firewalls' ease of management and performance." They also liked the Fortinet licensing model.

"Fortinet offers the hardware as it is," Mogelinski says. "You can plug in to any of the interfaces and expect to get whatever throughput the datasheet says. Unlike some of Fortinet's competitors, which require you to buy additional licensing for the firewalls to reach their full capability, you do not have to have a second tier of licensing to reach the published speeds of the FortiGate."

All in all, this first experience with FortiGates "opened our eyes," Mogelinski adds. "We said, 'If we are getting this much out of these devices, in this segment of the network, what happens if we add Fortinet solutions in other places?'"

## Nationwide Rip and Replace

A couple of years later, Mogelinski had the chance to answer that question, as the firewalls and software-defined wide area network (SD-WAN) throughout USI's many offices needed a refresh. The complexity of the legacy infrastructure put a perpetual strain on the network engineering group. They liked the idea of consolidating SD-WAN networking and security in a single device at each location.

Plus, Mogelinski asserts: "We already knew how well the FortiGates were securing the headends. We implicitly trusted that technology to protect our offices as well. We were somewhat invested in the legacy product, but we decided to switch to Fortinet and start fresh. We did a proof of concept for Fortinet Secure SD-WAN, and everybody at USI agreed that transitioning the entire WAN infrastructure to FortiGates was a no-brainer."

The rollout itself proved the wisdom of that decision. USI standardized on a single firewall model with a cable modem and multiprotocol label switching (MPLS) connectivity. Mogelinski and his team built a tool to customize the firewalls' configuration. "Once we finished our proof of concept, we had a 'golden template,'" he says. "We used the configuration generator tool to plug in variables that differed from site to site, like IP address. Then the tool would generate a configuration for the firewall in the form of two files that we saved to a USB drive."

USI engaged a Fortinet technical account manager (TAM) for a year to support the rollout. "He hopped in right away and reviewed our SD-WAN design and configurations," Mogelinski says. "Within an hour, he was rattling off best practices that we had not included in the plan. He quickly became like part of our team. In fact, he was so helpful that we just renewed the TAM agreement for five more years."

Once deployment got underway, the SD-WAN project proceeded very quickly. When a firewall arrived at a USI office, an operations staff member would fly or drive there with the appropriate USB stick. "They would plug the USB stick in to the new firewall, power it on, and in less than 10 minutes, the FortiGate was functional," Mogelinski says. "The on-site folks would log off. The operations team member would literally move three cables from the old firewall to the FortiGate, and that was it. The process was seamless, and the downtime was well under five minutes per site."

Within two months, all the company's sites had been converted to FortiGate. "It is incredible, when you pick the right technology, how quickly and easily you can make it work," Mogelinski adds.

[1] Region Stockholm: Sweden's Largest Health Provider Secures its Services with Increased Performance and Reliability at Lower Cost, Fortinet, accessed May 22, 2025.

[2] IHG Hotels & Resorts: IHG Hotels & Resorts Boosts IT Efficiency Close to 60% with Fortinet Secure SD-WAN, Fortinet, accessed May 22, 2025.

[3] Fordham University: Fordham University Reduces Staff Management Time by Over 50% with the Fortinet Security Fabric, Fortinet, accessed May 22, 2025.





June 3, 2025 2:00 PM / MKTG-1503-0-0-EN