Data Center Firewall Toolkit

FORTINET

Table of Contents

CHECKLIST

Top 5 Reasons to Choose a Fortinet Data Center Firewall

Digital transformation has significantly impacted the business world, enabling 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 data center security crucial for organizational success. Fortinet offers a comprehensive portfolio of data center cybersecurity solutions, including high-performance network protection through FortiGate Next-Generation Firewalls running on FortiOS. Here are five reasons to choose a Fortinet firewall for your data center.

☑ 1. Increased Performance

Fortinet is the only provider that employs patented ASIC technologies rather than the general-purpose processors used by most firewall vendors. This industry-exclusive approach increases the performance and throughput of FortiGate firewalls, which means faster and more accurate detection of today's threats, even for encrypted data and streaming video, resulting in a more secure network.

☑ 2. Improved Protection

The FortiGuard AI-Powered Security Suite is a comprehensive security solution that leverages artificial intelligence (AI) and machine learning (ML) to provide advanced threat protection. It provides market-leading security capabilities designed to protect application content, web traffic, devices, and users wherever they have been deployed. It continuously assesses risks and automatically responds to—and counters—known and unknown threats detected anywhere across the distributed network. Its coordinated and consistent real-time services defend against even the most sophisticated, evasive attacks, and its flexible form factors mean it can be deployed close to protected assets to ensure rapid, real-time detection and response.

☑ 3. One Operating System Enables Unification

The Fortinet Security Fabric is powered by FortiOS, a unified security and management framework that supports all form factors and can be deployed at all edges to consistently support and coordinate hybrid environments. This unique approach enables organizations to consolidate critical security and networking capabilities, ensuring direct access to application and data center resources.

☑ 4. Built with Sustainability in Mind

Environmentally responsible customers can be assured of our commitment to the environment. Fortinet's low-power cybersecurity network solution helps enterprises save on energy consumption, heat dissipation, and space, reducing their 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 consume less power to generate 1G of firewall throughput than our competitors for cleaner deployments.

5. Better ROI Than Rrivals

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:

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

Stay protected by eliminating security gaps in your network thanks to faster throughput and increased performance coupled with a single operating system that can implement security policies across all security devices on a network. Mix in the FortiGuard AI-Powered Security Suite that provides advanced threat protection for businesses for the industry's most powerful cybersecurity solution. And enjoy this increased performance while being environmentally friendly with our low power consumption data center firewalls. All this while achieving maximum ROI.

INDUSTRY INSIGHTS

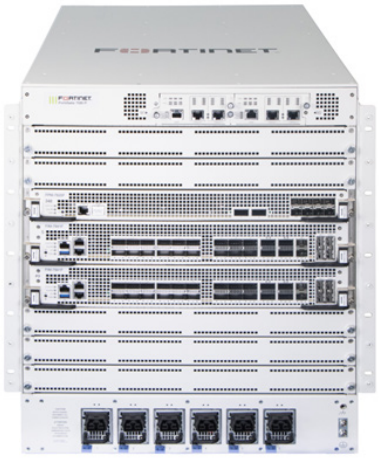
Boost Your Data Center's Performance and Security with FortiGate 7000F Series

The Most Comprehensive Data Center Security Solution

What Is a Hybrid Mesh Firewall?

Data centers are in the midst of an evolution. Physical, virtual, and cloud infrastructures are converging and changing the nature of on-premises data centers. Some believe this trend toward hybrid networks spells the end of the data center as well as traditional data center security—but they are far from dead.

A data center will always be an important element of any architecture. Therefore, fortifying data centers remains as vital as ever. To secure the modern evolving data center, Fortinet has the industry's most comprehensive data center cybersecurity solution. It's called FortiGate 7000F Series Next-Generation Firewall (NGFW) and it offers increased threat protection, performance, and energy efficiency.



FG-7000F Series NGFW

Significantly Better Than the Industry Standard

The FortiGate 7000F Series sets the standard for comprehensive data center security that protects mission-critical data across hybrid IT infrastructure. Performance and security are the two pillars of any NGFW, and, compared to the industry standard, the FortiGate 7000F Series delivers a security compute rating of:

- 5x NGFW performance
- 2x better threat protection
- 2x IPSec VPN throughput

Also, FortiGate 7000F Series is 73% more energy efficient per Gbps of firewall throughput compared to the industry standard. (To learn more about how our FortiGates compare to competing products, read the blog titled: Benchmarking Security Performance with Fortinet's Security Compute Ratings.)

Fortinet Security Compute Rating Table

Specification	FortiGate 7080F	Secure 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	4.1x	76.8	123.6	30	-	-
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

Like all FortiGate NGFWs, the FortiGate 7000F Series eliminates point products, reduces complexity, and enables the industry's best performance and return on investment (ROI).

Since our beginning, Fortinet has designed and built security devices so that they never become a performance bottleneck. The FortiGate 7000F Series continues to follow that founding principle, delivering 1.2 Tbps of firewall throughput coupled with 312 Gbps of threat protection—using 60% fewer watts of Gbps threat protection compared to the industry average.

Scaling without disrupting operations is a concern for many organizations, which is why the FortiGate 7000F Series was built to reduce the need for point products and simplify operations. It includes a high-power, energy-efficient eight-slot chassis that can house up to six Fortinet Processor Modules (FPMs) and includes 400GE ports that empower businesses to meet their evolving needs. (Fortinet remains the only firewall vendor to offer 400GE ports.)

The ASIC Advantage

Like all FortiGate solutions, the cornerstone of the FortiGate 7000F Series's performance and power savings is proprietary ASIC security processing units (SPU) specifically engineered for security and networking purposes.

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.

Accelerating 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 all-new 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 is a single operating system that provides centralized and unified management and visibility across the network.
- FortiGuard AI-Powered Security Services, developed by FortiGuard Labs (the Fortinet elite cybersecurity research organization), counter 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.
- 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.

Hybrid Mesh Firewall Ready

As businesses increasingly turn to hybrid environments to address the rise in cloud-based applications and remote workforces, it's critical for NGFWs, including solutions like the FortiGate 7000F Series, 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 and 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 web page.

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 hybrid clouds. However, to meet the needs of organizations expanding their digital transformation, the underlying enabling technologies must be more reliable, energy-efficient, and secure than ever.

Here are six things organizations need to do to position themselves for success:

☑ 1. Invest in a Flexible Next-Generation Firewall

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

☑ 2. Deploy Unified Networking and Security

Security can't be an afterthought. When security solutions are not well-integrated with one another or the underlying network, security risks and gaps arise as the attack surface expands and adapts. These blind spots are vulnerable to sophisticated multistep attacks and are partly responsible for the dramatic rise in successful ransomware attacks. As a result, it is essential to look for a unified security framework to deliver automated and reactive security that spans the entire attack surface. Organizations must also converge their security with networking to protect digital acceleration efforts.

☑ 3. Adopt a Secure-Networking Strategy

With new network edges being created on-premises and in the cloud, this unified convergence of networking and security must be available everywhere. And it must also be combined with zero-trust network access (ZTNA) to enable explicit access for applications and continuous verification of users and devices. This convergence is at the heart of a secure networking strategy. And flexible options for providing this convergence are also crucial in securing the digital acceleration of hybrid deployments.

☑ 4. 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 and tasks performed manually degrade the end-to-end digital experience. These issues increase the time to configure, manage, and troubleshoot. They also add to operations costs and errors that can cause network outages and reduce flexibility. With centralized and automated management and a dashboard able to span the whole network and security stack, the delivery of network services across their entire life cycle is expedited. Removing manual configuration eliminates a significant cause of downtime and security breaches.

5. Increase Visibility with End-to-End Digital Experience Monitoring

Traditional network, IT infrastructure, 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 customers need. They also severely hinder the visibility that frontline NOC and help desk teams need to resolve issues. A powerful digital experience monitoring (DEM) platform is required to give your NOC team superior visibility. It allows for observing 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.

6. Consolidate and Simplify Operations to Provide Instant ROI

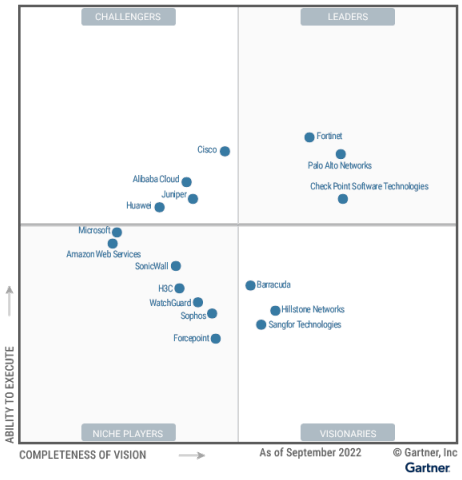
Organizations adopting modern networking technologies with integrated security achieve better ROI than point products with limited security. Secure networking also improves employee productivity with better user experience and simplified operations.

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 Software-as-a-Service (SaaS) environments, this legacy network design is an obstacle to 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.

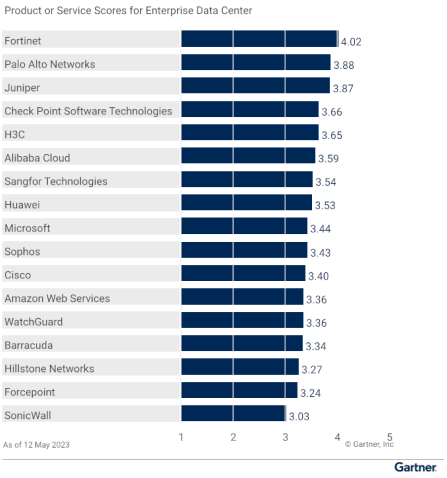
Third-Party Validation

Dec 2022 Gartner® Magic Quadrant for Network Firewalls



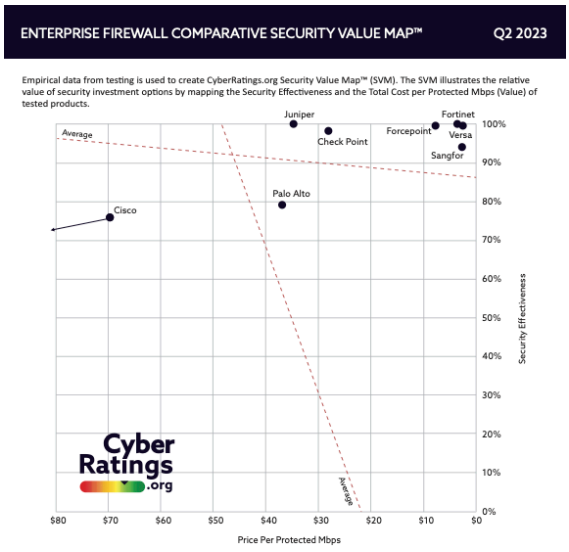
Fortinet named a leader positioned highest in Ability to Execute. This marks the 13th time Fortinet has been included in this Magic Quadrant™

May 2023 Gartner® Critical Capabilities for Network Firewalls



Ranked #1 for the Enterprise Data Center Use Case for Four Times in a row

Apr 2023 CyberRatings Enterprise Firewall Report



- 99.88% Security Effectiveness
- Recommended Rating
- Highest ROI among major players
- "AAA" Rating across all Categories

Oct 2022 Forrester Wave™ Enterprise Firewalls

Fortinet Named a Leader in the Forrester Wave.™

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

Gartner, Critical Capabilities for Network Firewalls, Adam Hils, Rajpreet Kaur, Thomas Lintemuth, 16 May 2023.

FORTINET

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 the delivery of 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 in size 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, the top cybersecurity priority for Mogelinski and his team 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 Next-Generation Firewalls (NGFWs), the legacy edgesecurity solution, and another competitor.

"We had a bake-off among the three heavy hitters from the Network Firewall Analyst Report. We weighed all the pros and cons. We ended up replacing our legacy firewalls with FortiGates, and once we deployed the Fortinet solutions, we fell in love."

Joe Mogelinski
Senior Network Engineer,
USI Insurance Services

Details

Customer:
USI Insurance Services

Industry: Insurance

Headquarters:
Valhalla, New York

Number of Secure SD-WAN Locations: 182

"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 into 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 FortiGates' published speeds."

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 WAN (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 SDWAN 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."

Business Impact

- WAN downtime cut in half: From around 40 outages per year to fewer than 20.
- Internet connectivity up to 10x faster from office locations
- Network engineering team can focus on more value-added activities due to networking and security solutions' ease of management
- Less than five minutes of office downtime to roll out a new firewall
- $1 million a year in savings on WAN hardware and support

Products and Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer
- FortiSIEM

Services

- FortiCare Professional Services
- FortiCare Technical Account Manager

FortiGuard Security Services

- Antivirus
- Virus Outbreak Protection Service
- Intrusion Prevention System
- Anti-malware

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 into 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.

> *"It is incredible when you pick the right technology how quickly and easily you can make it work"*
>
> **Joe Mogelinski**
> Senior Network Engineer,
> USI Insurance Services

FORTINET

www.fortinet.com

August 3, 2023 12:48 PM

2164008-0-0-EN