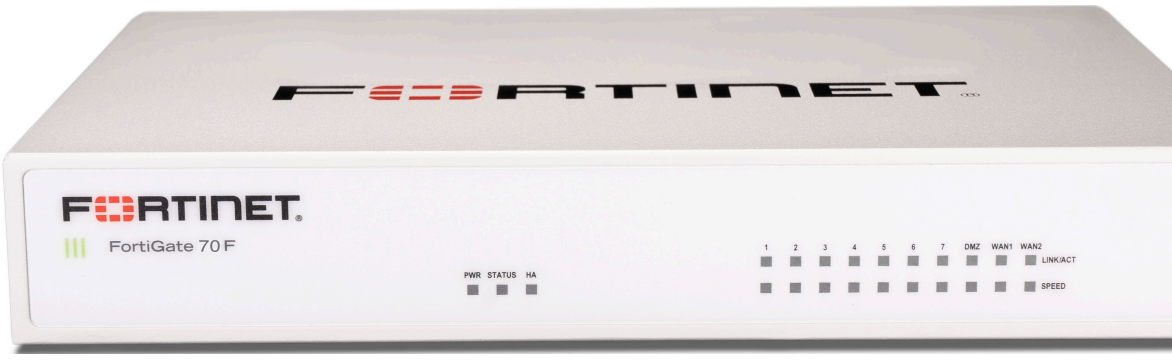
FortiGate 70F Series



Highlights

Gartner® Magic Quadrant™ Leaders for both Network Firewalls and SD-WAN

Unparalleled performance enabled by Fortinet's patented ASIC and the FortiOS operating system

Enterprise-grade protection with FortiGuard AI-Powered Security Services

Simplified operations with centralized management for networking and security, automated workflows, deep analytics, and self-healing

Inclusive SD-WAN and wireless controller in every FortiGate appliance at no extra cost

Rich portfolio for any business budget and need

Converged Next-Generation Firewall and SD-WAN

The FortiGate 70F series integrate firewalling, SD-WAN, and security in one appliance, making them perfect for building secure networks at distributed enterprise sites and transforming WAN architecture at any scale.

The 70F series is powered by FortiOS, the industry's first converged networking and security operating system. This convergence enables businesses to efficiently and optimally secure today's dynamic digital infrastructures.

As a cornerstone of the Fortinet Security Fabric platform, the FortiGate NGFW works seamlessly with FortiGuard AI-Powered Security Services to deliver coordinated, automated, end-to-end threat protection in real time.

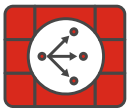
The 70F family is built on the patented SD-WAN-based ASIC, which delivers unmatched performance over traditional CPUs with lower cost and reduced power consumption. This application-specific design and embedded multi-core processor further accelerate the convergence of networking and security functions in the 70F family to optimize secure connections and deliver a robust user experience at branch locations.

IPS	NGFW	Threat Protection	Interfaces
1.4 Gbps	1 Gbps	800 Mbps	Multiple GE RJ45 | Variants with internal storage

Use Cases

Perimeter Protection

- Protect networks from malicious traffic, guard against file-based threats, block web-based attacks, and secure applications and data with natively integrated FortiGuard AI-Powered Security Services
- Inspect and control incoming and outgoing traffic based on defined security policies
- Perform real-time SSL inspection (including TLS 1.3) with full visibility into users, devices, and applications across the attack surface
- Accelerate performance, protection, and energy efficiency with Fortinet's patented SPU with converged security and networking technologies



Secure SD-WAN

- FortiGate enables best-of-breed WAN edge with integrated SD-WAN, WAN optimization, security, and unified management from a single FortiOS operating system
- FortiGate, built on a patented SD-WAN-based ASIC, delivers faster application identification to avoid delays in accessing applications and accelerates overlay performance regardless of location
- Enhances hybrid working with a comprehensive SASE solution by integrating cloud-delivered SD-WAN with security service edge (SSE)
- Achieves operational efficiencies at any scale through automation, deep analytics, and self-healing

Secure Branch

- The Fortinet Security Fabric platform enables FortiGate NGFWs to automatically discover and secure IoT devices for faster branch onboarding
- Fully integrated with FortiSwitch secure Ethernet switches and FortiAP access points, FortiGate easily extends security to WAN, LAN, and WLAN at branch offices for unified protection and reliable connectivity
- FortiGate and Fortinet products work seamlessly with FortiManager to centralize visibility and simplify management across locations for IT teams
- FortiGate HA support ensures continuous network protection and minimizes downtime in the event of hardware failures or network disruptions

Universal ZTNA

Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies.

- Provide extensive authentications, checks, and enforce policy prior to granting application access every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Infused with the latest threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero-day and sophisticated AI-powered attacks.

Network and file security

Network and file security services protect against network and file-based threats. With over 18,000 signatures, our industry-leading intrusion prevention system (IPS) uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, and applying virtual patches for newly discovered vulnerabilities. Anti-malware protection defends against both known and unknown file-based threats, combining antivirus and sandboxing for multi-layered security. Application control improves security compliance and provides real-time visibility into applications and usage.

Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of over 300 million URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks. FortiGuard Labs blocks over 500 million malicious/phishing/spam URLs weekly, and blocks 32,000 botnet command-and-control attempts every minute, demonstrating the robust protection offered through Fortinet.

SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This includes data loss prevention to ensure visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. Our inline cloud access security broker service protects data in motion, at rest, and in the cloud, enforcing compliance standards and managing account, user, and cloud app usage. Services also assess infrastructure, validate configurations, and highlight risks and vulnerabilities, including IoT device detection and vulnerability correlation.

Zero-Day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown malware in real time, delivering sub-second protection across all NGFWs. The service also integrates the MITRE ATT&CK matrix to speed up investigations. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

OT security

With over 1000 virtual patches, 1100+ OT applications, and 3300+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Real-Time Network Security Operating System

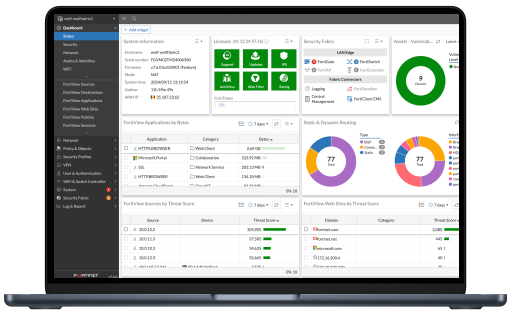
FortiOS is the operating system that powers Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. FortiOS provides a unified framework for managing and securing networks, cloud-based, hybrid, or a convergence of IT, OT, and IoT. FortiOS enables seamless and efficient interoperation across Fortinet products with consistent and consolidated AI-powered protection across today's hybrid environments.

Unlike traditional point solutions, Fortinet adopts a holistic approach to cybersecurity, aiming to reduce complexities, eliminate security silos, and improve operational efficiencies. By consolidating security functions into a single platform, FortiOS simplifies management, reduces costs, and enhances overall security posture. Together, FortiGate and FortiOS create intelligent, adaptive protection to help organizations reduce complexity, eliminate security silos, and optimize user experience.

By integration generative AI (GenAI), FortiOS further enhances the ability to analyze network traffic and threat intelligence, detects deviations or anomalies more effectively, and provides more precise remediation recommendations, ensuring minimum performance impact without compromising security.

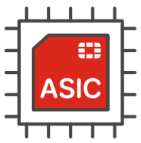
Learn more about what's new in FortiOS. https://www.fortinet.com/products/fortigate/fortios

Intuitive easy to use view into the network and endpoint vulnerabilities



Comprehensive view of network performance, security, and system status

Fortinet ASICs: Unrivaled Security, Unprecedented Performance



Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

Secure SD-WAN ASIC SP4

- Combines a RISC-based CPU with Fortinet's proprietary SPU content and network processors for unmatched performance
- Delivers the industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for the best user experience on direct internet access
- Enables best-of-breed NGFW security and deep SSL inspection with high performance
- Extends security to the access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

Unified Management for Optimal Security and Efficiency

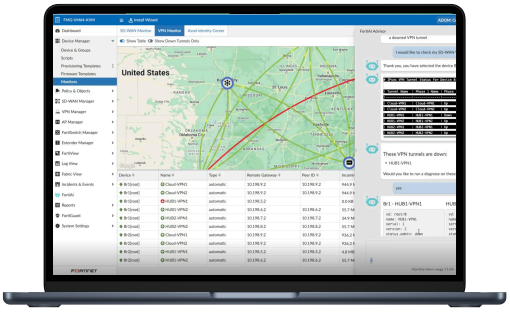
Whether you are a small business or a large enterprise, Fortinet provides centralized control, visibility, and automation for your security infrastructure.

FortiManager: Centralized management at scale for distributed enterprises

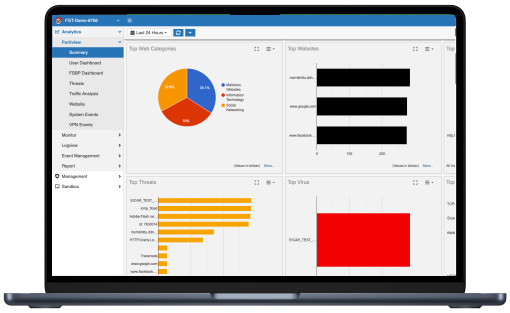
FortiManager, powered by FortiAI, is a centralized management solution for the Fortinet Security Fabric. It streamlines mass provisioning and policy management for FortiGate, FortiGate VM, cloud security, SD-WAN, SD-Branch, FortiSASE, and ZTNA in hybrid environments. Additionally, FortiManager provides real-time monitoring of the entire managed infrastructure and automates network operation workflows. Leveraging GenAI in FortiAI, it further enhances Day 0–1 configurations and provisioning, and Day N troubleshooting and maintenance, unlocking the full potential of the Fortinet Security Fabric and significantly boosting operational efficiency.

FortiGate Cloud: Simplified management for small and mid-size businesses

FortiGate Cloud is a SaaS service offering simplified management, security analytics, and reporting for Fortinet FortiGate NGFWs to help you more efficiently manage your devices and reduce cyber risk. It simplifies the initial deployment, setup, and ongoing management of FortiGates and downstream connected devices such as FortiAP, FortiSwitch, and FortiExtender, with zero-touch provisioning. It provides real-time and historical visibility into traffic analytics and security threats to reduce risks and improve security posture. View various threats, web traffic, and system events stored in the cloud for up to a year, with predefined reports to meet compliance and deliver actionable insights.



GenAI in FortiManager helps manage networks effortlessly—generate configuration and policy scripts, troubleshoot issues, and execute recommended actions.



FortiGate Cloud provides intuitive management and analytics solution with end-to-end visibility, logging and reporting for SMB.

FortiConverter Service

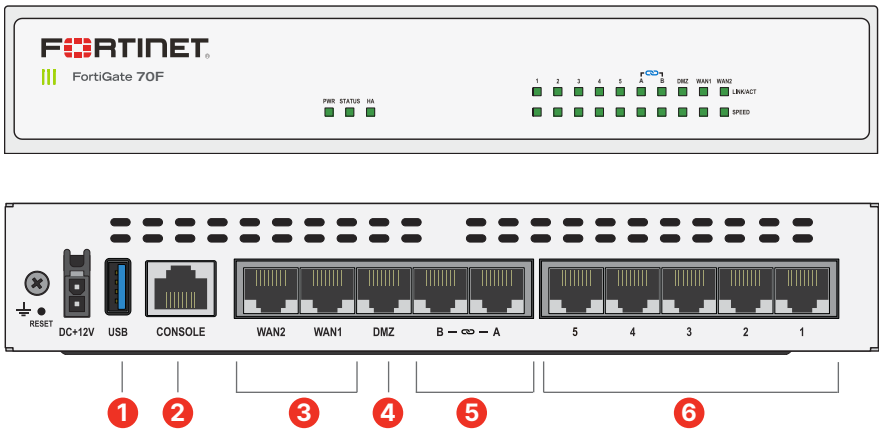
Migration to FortiGate NGFW made easy

The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

Hardware

FortiGate 70F/71F

SoC4 DESKTOP 128GB



Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 WAN Ports
4. 1 x GE RJ45 DMZ Port
5. 2 x GE RJ45 FortiLink Ports
6. 5 x GE RJ45 Internal Ports

Hardware Features

Access layer security

FortiLink protocol enables you to converge security and network access by integrating the FortiSwitch into the FortiGate as a logical extension of the firewall. These FortiLink-enabled ports can be reconfigured as regular ports as needed.

Compact and reliable form factor

Designed for small environments, the FortiGate can be on a desktop or wall-mounted. It is small, lightweight, yet highly reliable with superior meantime between failures, minimizing the chance of network disruption.

Specifications

	FORTIGATE 70F	FORTIGATE 71F
Hardware Specifications		
GE RJ45 WAN / DMZ Ports	2 / 1	2 / 1
GE RJ45 Internal Ports	5	5
GE RJ45 FortiLink Ports (Default)	2	2
Wireless Interface	–	–
USB Ports	1	1
Console (RJ45)	1	1
Internal Storage	–	1 × 128 GB SSD
Trusted Platform Module (TPM)	—	—
Bluetooth Low Energy (BLE)	—	—
Signed Firmware Hardware Switch	—	—
System Performance* — Enterprise Traffic Mix		
IPS Throughput [2]	1.4 Gbps	
NGFW Throughput [2, 4]	1 Gbps	
Threat Protection Throughput [2, 5]	800 Mbps	
System Performance and Capacity		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10/10/6 Gbps	
Firewall Latency (64 byte UDP packets)	2.54 µs	
Firewall Throughput (Packets Per Second)	9 Mpps	
Concurrent Sessions (TCP)	1.5 M	
New Sessions/Second (TCP)	35 000	
Firewall Policies	5000	
IPsec VPN Throughput (512 byte) [1]	6.1 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	200	
Client-to-Gateway IPsec VPN Tunnels	500	
SSL-VPN Throughput	405 Mbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	700 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	100 000	
Application Control Throughput (HTTP 64K) [2]	1.8 Gbps	
CAPWAP Throughput (HTTP 64K)	8.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	24	
Maximum Number of FortiAPs (Total / Tunnel Mode)	64 / 32	
Maximum Number of FortiTokens	500	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 70F	FORTIGATE 71F
Dimensions		
Height x Width x Length (inches)	1.5 × 8.5 × 6.3	
Height x Width x Length (mm)	38.5 × 216 × 160 mm	
Weight	2.23 lbs (1.01 kg)	
Form Factor	Desktop	
Operating Environment and Certifications		
Power Rating	12VDC, 3A	
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz	
Maximum Current	100VAC/1.0A, 240VAC/0.6A	
Power Consumption (Average / Maximum)	10.17 W / 12.43 W	17.2 W / 18.7 W
Heat Dissipation	63.1 BTU/hr	63.8 BTU/hr
Operating Temperature	32°F to 104°F (0°C to 40°C)	
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	
Humidity	Humidity 10% to 90% non-condensing	
Noise Level	Fanless 0 dBA	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Certifications	USGv6/IPv6	

Note: All performance values are “up to” and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct [3], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video [3] Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention [3]	•	•		
	Data Loss Prevention (DLP) [1]	•	•		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	•	•		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS [1]	•			
	Application Control		included with FortiCare Subscription		
	Inline CASB [3]		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring	•			
	SD-WAN Overlay-as-a-Service	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth) [2]	•			
NOC and SOC Services	FortiConverter Service for one time configuration conversion	•	•		
	Managed FortiGate Service—available 24×7, with Fortinet NOC experts performing device setup, network, and policy change management	•			
	FortiGate Cloud—Management, Analysis, and One Year Log Retention	•			
	FortiManager Cloud	•			
	FortiAnalyzer Cloud	•			
	FortiGuard SOCaaS—24×7 cloud-based managed log monitoring, incident triage, and SOC escalation service	•			
Hardware and Software Support	FortiCare Essentials [2]	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing		included with FortiCare Subscription		

1. Full features available when running FortiOS 7.4.1.
2. Desktop Models only.
3. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards.

FortiGuard AI-Powered Security Bundles for FortiGate

FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24×7×365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.

FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an extended end-of-engineering support of 18 months, providing flexibility and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

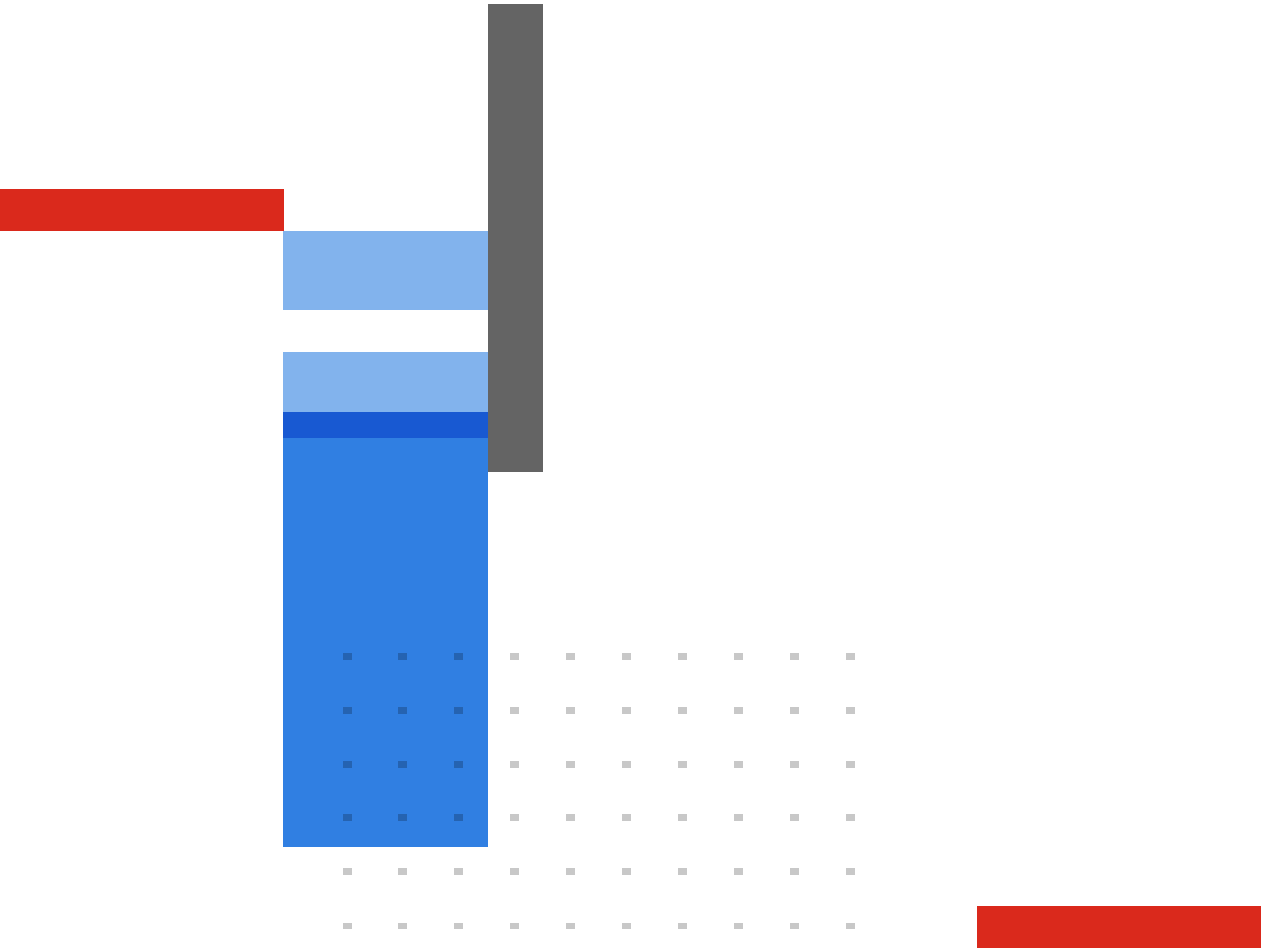
Ordering Information

Product	SKU	Description
FortiGate 70F	FG-70F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port).
FortiGate 71F	FG-71F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage.
Optional Accessories		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01.
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, FG/FWF 60F/61F, FG-70F/71F, and FG-80E/81E.
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-60F, FG-70F/71F and FG/FWF-80F series.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

Copyright © 2024 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 SVP Legal and above, 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.

October 4, 2024

FG-70F-DAT-R10-20241004