FortiGate 40F Series



Highlights

Leader in the Gartner® Magic Quadrant™ for Hybrid Mesh Firewall

Unparalleled performance enabled by Fortinet's patented ASIC and the AI-enriched 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 network 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 40F series integrates firewalling, SD-WAN, network controller, and security in one appliance, making them perfect for building secure networks at distributed enterprise sites and transforming WAN architecture at any scale.

The 40F series runs on FortiOS, a converged networking and security platform with secure AI controls and quantum-safe protection. This single OS approach enables businesses to gain benefits of operational efficiency and unified protection from the seamless integration of Fortinet solutions within a hybrid mesh firewall architecture.

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 40F 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 40F family to optimize secure connections and deliver a robust user experience at branch locations.

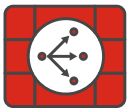
IPS	NGFW	Threat Protection	Interfaces
1 Gbps	800 Mbps	600 Mbps	Multiple GE RJ45 | WiFi variants

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

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

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

FortiOS is Fortinet's natively AI-powered and quantum-safe operating system (OS) that powers the Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. It provides a unified framework for securing networks across on-premises, cloud, hybrid environments, and the convergence of IT, OT, and IoT.

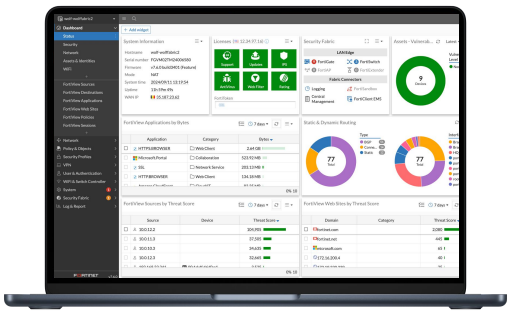
By converging networking and security functions into a single operating system, organizations can manage network and security more effectively to detect, investigate, and respond to incidents faster. This unified architecture simplifies operations, eliminates security silos, and allows organizations to scale securely without multiple tools or management complexity.

FortiOS also incorporates AI-driven capabilities that enhance threat detection, automate network activity analysis, and deliver more precise remediation guidance. Together, FortiGate firewalls and FortiOS provide intelligent, adaptive protection that reduces complexity, improves operational efficiency, and strengthens security across modern hybrid environments.

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



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. Powered by real-time AI enhanced threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero days and evasive, sophisticated AI-powered attacks.

Network and file security

Network and file security services protect against network and file-based threats. Consists of intrusion prevention system (IPS) which uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, uncovers hidden command-and-control activity, and applies virtual patches for newly discovered vulnerabilities. Application control improves security compliance and provides real-time visibility into applications and usage including generative AI (GenAI) applications.

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 millions of URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks.

SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This service includes data loss/leakage prevention in files, GenAI applications and Images via OCR (optical character recognition). This ensures visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. The inline CASB service, secures SaaS applications in use, providing broad visibility and granular control over SaaS access, usage, and data.

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 and zero-day malware in real time, delivering sub-second protection across all NGFWs. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

Attack surface visibility and compliance

The FortiGuard Attack Surface Security Service provides continuous, compliance-ready monitoring of your Fortinet Security Fabric infrastructure. It calculates your overall security posture rating by scoring controls against vulnerabilities, misconfigurations, and sub-optimal settings, while offering specific remediation guidelines for devices found out of configuration. It maintains continuous compliance with PCI DSS, CIS Controls, and Fortinet security best practices.

OT security

With over 2400 virtual patches, 1600+ OT applications, and 3500+ 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.

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: AI-powered, automation-driven, enterprise-class centralized management at scale

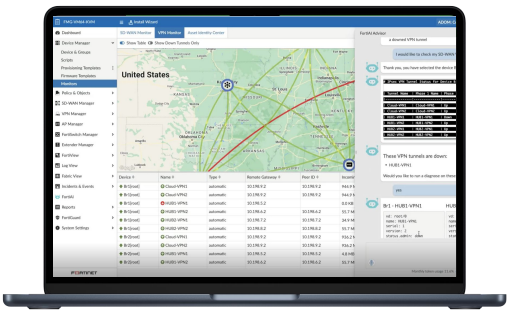
FortiManager, powered by FortiAI-Assist, provides centralized, single-pane management for the Fortinet Security Fabric, unifying configuration, policy, and responses across thousands of devices. It converges networking and security management, enabling consistent policy enforcement across SD-WAN, ZTNA, SASE, and branch environments while delivering real-time visibility and automated network operations.

FortiAI-Assist helps with Day 0–1 provisioning and Day N troubleshooting and maintenance. AI agents collaborating via a unified Model Context Protocol (MCP) framework automates goal-driven tasks toward a self-healing operation.

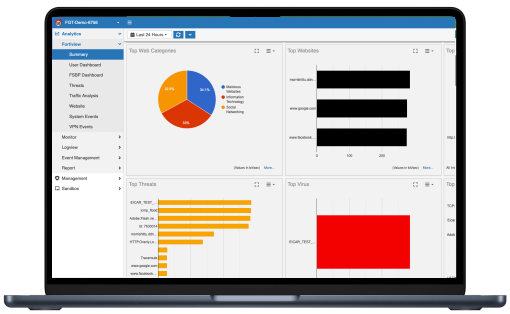
FortiManager integrates with FortiSOC for contextual insights and fabric-wise response. It also supports ecosystem integrations, and open APIs for extended automation. ADOM-based administration and FortiManager clusters enables resilient control across distributed networks.

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.



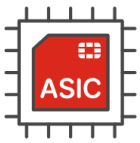
FortiGate Cloud provides intuitive management and analytics solution with end-to-end visibility, logging and reporting for SMB.

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.

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.

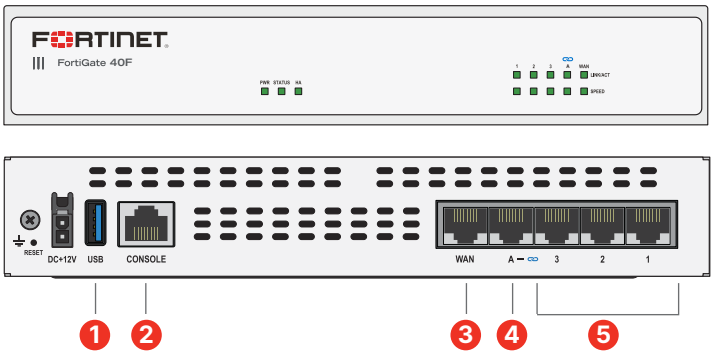
Secure SD-WAN ASIC SP4

- 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

Hardware

FortiGate 40F Series

SoC4 DESKTOP

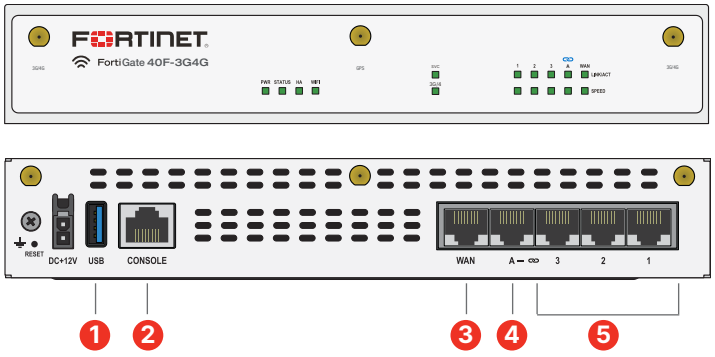


Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 1 x GE RJ45 WAN Port
4. 1 x GE RJ45 FortiLink Port
5. 3 x GE RJ45 Ethernet Ports

FortiGate 40F-3G4G

SoC4 DESKTOP 3G4G/LTE a/b/g/n/ac-W2



Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 1 x GE RJ45 WAN Port
4. 1 x GE RJ45 FortiLink Port
5. 3 x GE RJ45 Ethernet 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 40F	FORTIGATE 40F-3G4G
Interfaces and Modules		
Hardware Accelerated GE RJ45 WAN / DMZ Ports	1	1
Hardware Accelerated GE RJ45 Internal Ports	3	3
Hardware Accelerated GE RJ45 FortiLink Ports (Default)	1	1
Hardware Accelerated GE RJ45 PoE/+ Ports	0	0
Cellular Modem	—	3G4G LTE
Wireless Interface	0	0
Antenna Ports (SMA)	0	3
USB Ports	1	1
Console Port (RJ45)	1	1
SIM Slots (Nano SIM)	0	2
Onboard Storage	0	0
Included Transceivers	0	0
Trusted Platform Module (TPM)	—	—
Bluetooth Low Energy (BLE)	—	—
Signed Firmware Hardware Switch	—	—
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	1 Gbps	
NGFW Throughput [2, 4]	800 Mbps	
Threat Protection Throughput [2, 5]	600 Mbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	5 / 5 / 5 Gbps	
Firewall Latency (64 byte, UDP)	2.97 µs	
Firewall Throughput (Packet per Second)	7.5 Mpps	
Concurrent Sessions (TCP)	700 000	
New Sessions/Second (TCP)	35 000	
Firewall Policies	2000	
IPsec VPN Throughput (512 byte) [1]	4.4 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	200	
Client-to-Gateway IPsec VPN Tunnels	250	
SSL-VPN Throughput[6]	490 Mbps	
Concurrent SSL-VPN Users[6] (Recommended Maximum, Tunnel Mode)	200	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	310 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	320	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000	
Application Control Throughput (HTTP 64K) [2]	990 Mbps	
CAPWAP Throughput (HTTP 64K)	3.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	8	
Maximum Number of FortiAPs (Total / Tunnel)	16 / 8	
Maximum Number of FortiTokens	500	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

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.

[6] SSL VPN not supported on FortiOS 7.6.0 and above.

Specifications

	FORTIGATE 40F	FORTIGATE 40F-3G4G
Dimensions and Power		
Height x Width x Length (inches)	1.5 × 8.5 × 6.3	1.6 × 8.5 × 6.3
Height x Width x Length (mm)	38.5 × 216 × 160	40.5 × 216 × 160
Weight	2.2 lbs (1 kg)	2.2 lbs (1 kg)
Form Factor (supports EIA/non-EIA standards)	Desktop	Desktop
Input Rating	12Vdc, 3A	12Vdc, 3A
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz	Powered by external DC power adapter 100-240V AC, 50/60 Hz
Current (Maximum)	100V AC / 0.2A, 240V AC / 0.1A	100V AC / 0.3A, 240V AC / 0.2A
Power Consumption (Average / Maximum)	7.74 W / 9.46 W	15.8 W / 18.6 W
Heat Dissipation	52.55 BTU/h	63.5 BTU/h
Operating Environment and Certifications		
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	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	
Radio Specifications		
Multiple (MU) MIMO	N/A	N/A
Maximum Wi-Fi Speeds	N/A	N/A
Maximum Tx Power	N/A	N/A
Antenna Gain	N/A	N/A
3G4G Modem		
Maximum Tx Power	N/A	20 dBm
Regions	N/A	All Regions
Modem Model	N/A	Sierra Wireless EM7565 (2 SIM Slots, Active/Passive)
LTE Category	N/A	CAT-12
LTE Bands	N/A	B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B18, B19, B20, B26, B28, B29, B30, B32, B41, B42, B43, B46, B48, B66
UMTS/HSPA+	N/A	B1, B2, B4, B5, B6, B8, B9, B19
WCDMA	N/A	—
CDMA 1xRTT/EV-DO Rev A	N/A	—
GSM/GPRS/EDGE	N/A	—
Module Certifications	N/A	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB
Diversity	N/A	Yes
MIMO	N/A	Yes
GNSS Bias	N/A	Yes

EPD
INTERNATIONAL EPD SYSTEM

Third-party verified Environmental Product Declaration

The FortiGate 40F is EPD compliant with ISO 14025 Type III (externally verified), ensuring data accuracy and full transparency on the product environmental impacts throughout its life cycle. For more information please visit https://www.environdec.com/library/epd21558

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles			
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection	SD-WAN
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•	
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct[1], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•	
	URL, DNS and Video Filtering — URL, DNS and Video[1] Filtering, Malicious Certificate	•	•	•		
	Anti-Spam		•	•		
	AI-based Inline Malware Prevention	•	•			
	Data Loss Prevention (DLP) [2]	•	•			
	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 [2]	•				
	Application Control		----------included with FortiCare Subscription----------			
	Inline CASB[1]		----------included with FortiCare Subscription----------			
SD-WAN and SASE Services	SD-WAN SLA Database					•
	SD-WAN Underlay and Application Monitoring Service					•
	SD-WAN Overlay Orchestration Service					•
	SD-WAN Connector for FortiSASE Secure Private Access					•
	FortiSASE Starter Kit for n* Users[3]					•
	FortiGate Cloud One Year Cloud-based Log Retention					•
	FortiTelemetry Cloud					•
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	Desktop models only				
	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. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.
2. Full features available when running FortiOS 7.4.1.
3. Only supported on FortiGate models from the 100F onwards (F-series and all later series).
See the FortiSASE Ordering Guide for supported models and corresponding user license allocations.

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

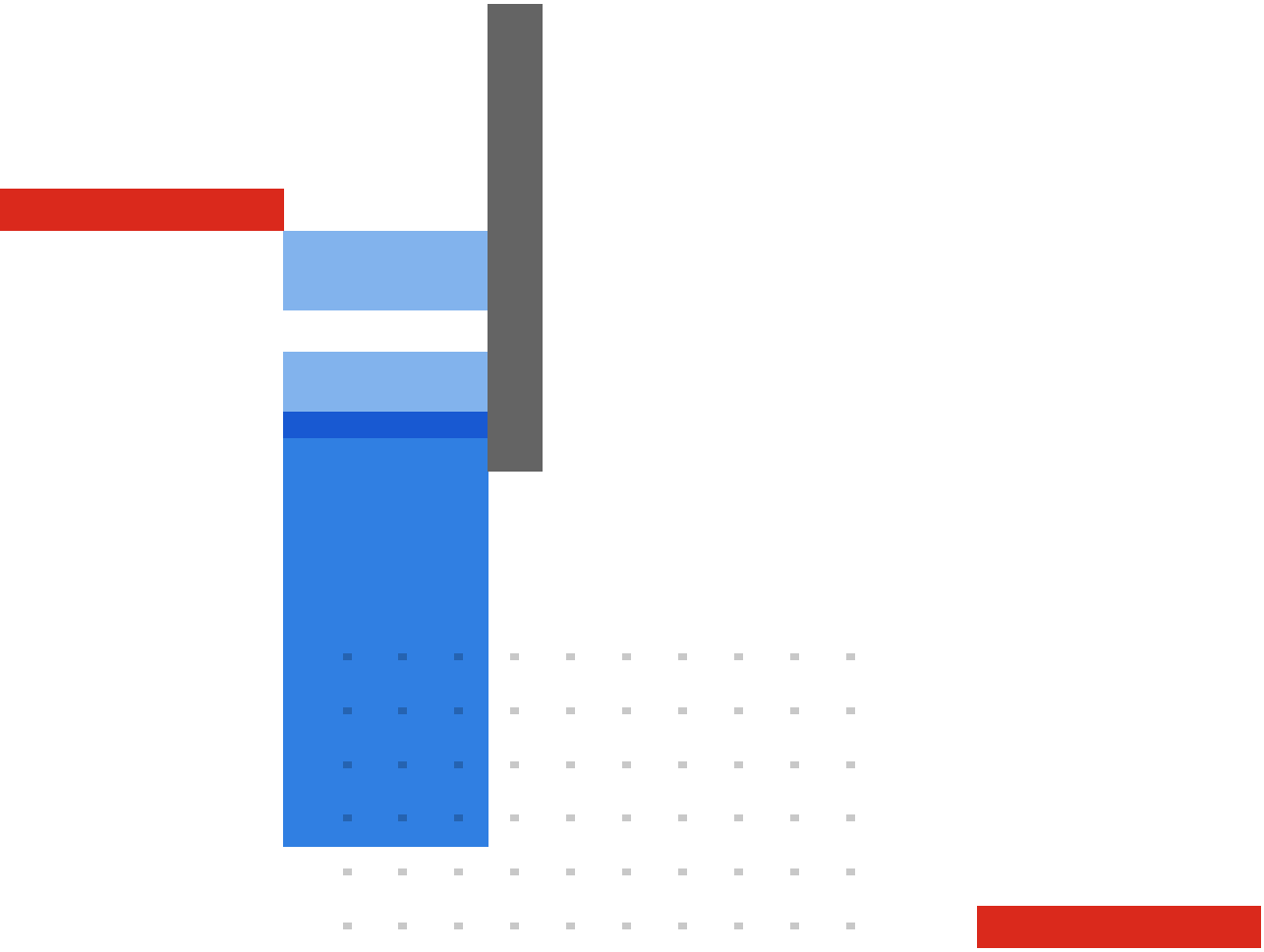
Product	SKU	Description
FortiGate 40F	FG-40F	5x GE RJ45 ports (including 4x Internal Ports, 1x WAN Ports).
FortiGate 40F	FG-40F-HA	5 x GE RJ45 ports (including, 1 x WAN Port, 4 x Internal Ports). FG-XX-HA SKUs must to be bought in pairs and entitle HA pair to leverage single service contracts.
FortiGate 40F-3G4G	FG-40F-3G4G	5x GE RJ45 ports (Including 1x WAN port, 4x Switch ports) with Embedded 3G/4G/LTE wireless wan module, external SMA WWAN antennas included.
FortiGate 40F-3G4G	FG-40F-3G4G-HA	5 x GE RJ45 ports (including 1 x WAN Port, 4 x Internal Ports) with Embedded 3G/4G/LTE wireless wan module, 3 external SMA WWAN antennas included. FG-XX-HA SKUs must to be bought in pairs and entitle HA pair to leverage single service contracts.
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. For list of compatible FortiGate products, visit our Documentation website, docs.fortinet.com
AC Power Adaptor	SP-FG-40F-PA-10(-XX)	Pack of 10 AC power adaptors for FG-40F, come with interchangeable power plugs. (XX=various countries code).
Wall Mount Kits	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG-40F series, FG/FWF-60F series, FG-80F, FG-81F and FG-80F-Bypass.

[RC] = regional code: A, B, D, E, F, I, J, N, P, S, V, and Y

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 © 2026 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.

April 21, 2026

FG-40F-DAT-R48-20260421