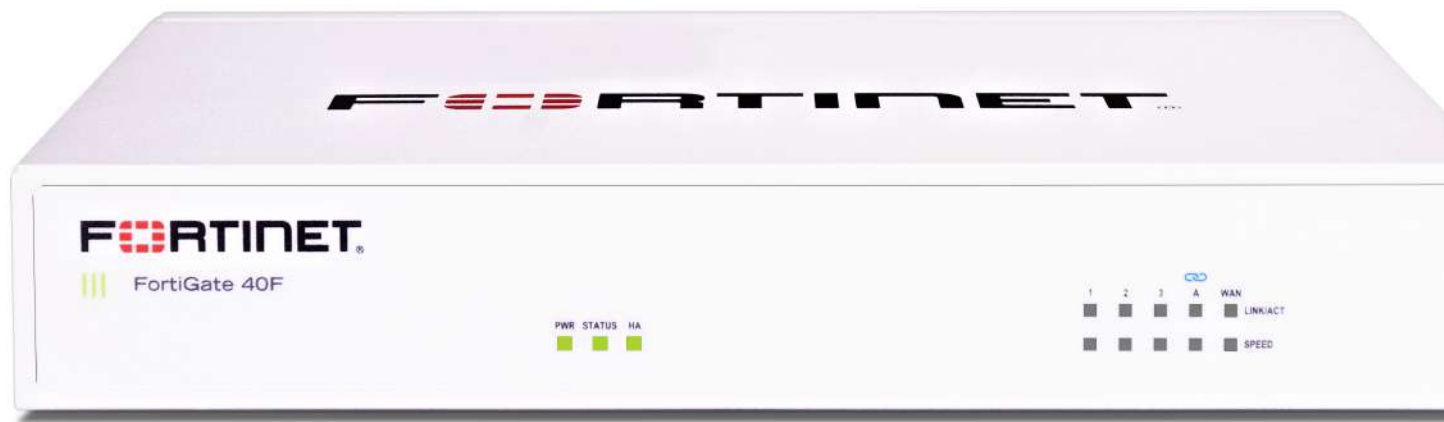# FortiGate FortiWiFi 40F Series

FG-40F, FG-40F-3G4G, FWF-40F, FWF-40F-3G4G

Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and SD-WAN.

Security-Driven Networking with FortiOS delivers converged networking and security.

Unparalleled Performance with Fortinet's patented SoC processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Simplified Operations with centralized management for networking and security, automation, deep analytics, and self-healing.

Converged Next-Generation Firewall (NGFW) and SD-WAN

The FortiGate Next-Generation Firewall 40F series is ideal for building security-driven networks at distributed enterprise sites and transforming WAN architecture at any scale.

With a rich set of AI/ML-based FortiGuard security services and our integrated Security Fabric platform, the FortiGate FortiWiFi 40F series delivers coordinated, automated, end-to-end threat protection across all use cases.

FortiGate has the industry's first integrated SD-WAN and zero-trust network access (ZTNA) enforcement within an NGFW solution and is powered by one OS. FortiGate 40F automatically controls, verifies, and facilitates user access to applications, delivering consistency with a seamless and optimized user experience.

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

FOS

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's advanced operating system

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into organically built best-of-breed capabilities, unified operating system, and ultra-scalability. The solution allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more. It provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of a simplified, single policy and management framework. Its security policies enable centralized management across large-scale networks with the following key attributes:

• Interactive drill-down and topology viewers that display real-time status

• On-click remediation that provides accurate and quick protection against threats and abuses

• Unique threat score system correlates weighted threats with users to prioritize investigations

*Intuitive easy to use view into the network and endpoint vulnerabilities*

Visibility with FOS Application Signatures

FortiConverter Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. 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.
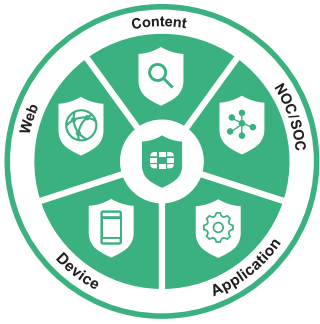
FortiGuard Services

FortiGuard AI-Powered Security

FortiGuard's rich suite of security services counter threats in real time using AI-powered, coordinated protection designed by FortiGuard Labs security threat researchers, engineers, and forensic specialists.

Web Security

Advanced cloud-delivered URL, DNS (Domain Name System), and Video Filtering providing complete protection for phishing and other web born attacks while meeting compliance.

Additionally, its dynamic inline CASB (Cloud Access Security Broker) service is focused on securing business SaaS data, while inline ZTNA traffic inspection and ZTNA posture check provide per-sessions access control to applications. It also integrates with the FortiClient Fabric Agent to extend protection to remote and mobile users.

Content Security

Advanced content security technologies enable the detection and prevention of known and unknown threats and file-based attack tactics in real-time. With capabilities like CPRL (Compact Pattern Recognition Language), AV, inline Sandbox, and lateral movement protection make it a complete solution to address ransomware, malware, and credential-based attacks.

Device Security

Advanced security technologies are optimized to monitor and protect IT, IIoT, and OT (Operational Technology) devices against vulnerability and device-based attack tactics. Its validated near-real-time IPS intelligence detects, and blocks known and zero-day threats, provides deep visibility and control into ICS/OT/SCADA protocols, and provides automated discovery, segmentation, and pattern identification-based policies.

Advanced Tools for SOC/NOC

Advanced NOC and SOC management tools attached to your NGFW provide simplified and faster time-to-activation.

SOC-as-a-Service

Includes tier-one hunting and automation, log location, 24×7 SOC analyst experts, managed firewall and endpoint functions, and alert triage.

Fabric Rating Security Best Practices

Includes supply chain virtual patching, up-to-date risk and vulnerability data to deliver quicker business decisions, and remediation for data breach situations.

Secure Any Edge at Any Scale
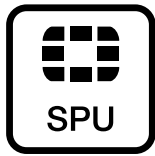
### Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

### ASIC Advantage

Secure SD-WAN ASIC SOC4

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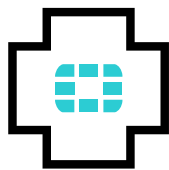
FortiCare Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.

Use Cases
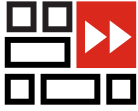
Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection

Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

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
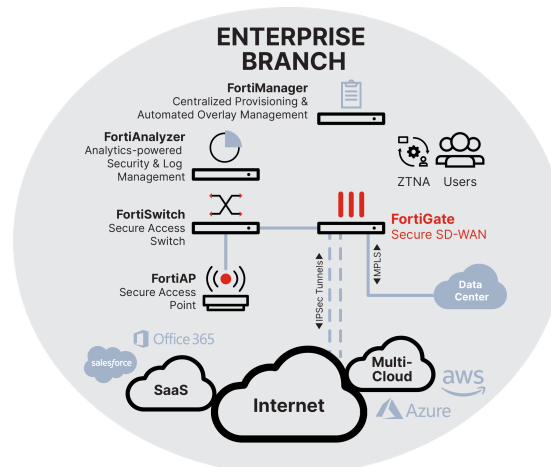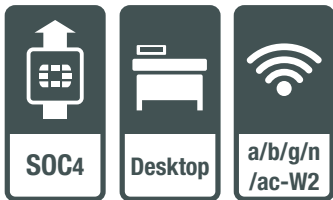
Hardware
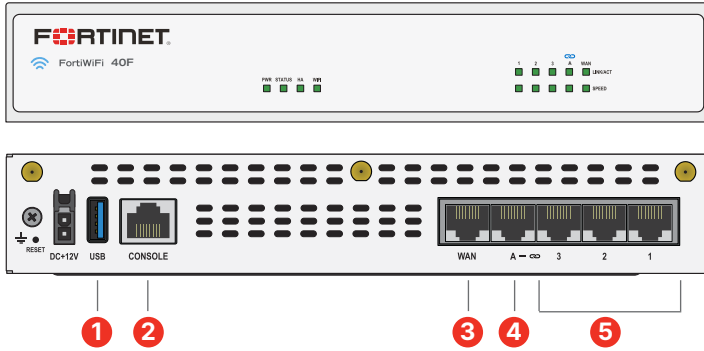
FortiGate FortiWifi 40F Series

FortiGate FortiWifi 40F-3G4G

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

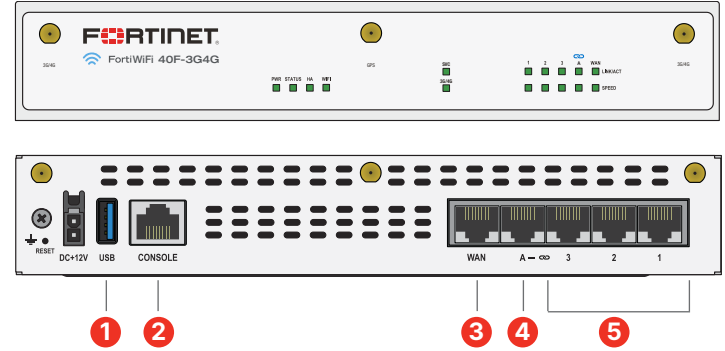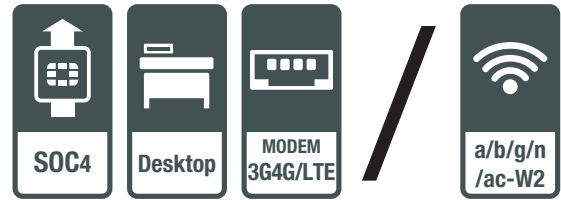### Hardware Features

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

Specifications

	FORTIGATE 40F	FORTIWIFI 40F	FORTIGATE 40F-3G4G	FORTIWIFI 40F-3G4G
Interfaces and Modules				
Hardware Accelerated GE RJ45 WAN / DMZ Ports	1	1	1	1
Hardware Accelerated GE RJ45 Internal Ports	3	3	3	3
Hardware Accelerated GE RJ45 FortiLink Ports (Default)	1	1	1	1
Hardware Accelerated GE RJ45 PoE/+ Ports	0	0	0	0
Cellular Modem	-	-	3G4G LTE	3G4G LTE
Wireless Interface	0	Single Radio (2.4GHz/5GHz) 802.11 /a/b/g/n/ac-W2	0	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2
Antenna Ports (SMA)	0	3	3	6
USB Ports	1	1	1	1
Console Port (RJ45)	1	1	1	1
SIM Slots (Nano SIM)	0	0	2	2
Onboard Storage	0	0	0	0
Included Transceivers	0	0	0	0
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	5000			
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	490 Mbps			
Concurrent SSL-VPN Users (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.

Specifications

	FORTIGATE 40F	FORTIWIFI 40F	FORTIGATE 40F-3G4G	FORTIWIFI 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	14.6 W / 16.6 W	15.8 W / 18.6 W	18.6 W / 19.8 W
Heat Dissipation	52.55 BTU/h	56.64 BTU/h	63.5 BTU/h	67.6 BTU/h
Operating Environment and Certifications				
Operating Temperature	32°–104°F (0°–40°C)			
Storage Temperature	-31°–158°F (-35°–70°C)			
Humidity	10%–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	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN			
Radio Specifications				
Multiple (MU) MIMO	N/A	3 × 3	N/A	3 × 3
Maximum Wi-Fi Speeds	N/A	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz	N/A	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz
Maximum Tx Power	N/A	20 dBm	N/A	20 dBm
Antenna Gain	N/A	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz	N/A	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz
Regional Compatibility				
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	

SUBSCRIPTIONS

Service Category	Service Offering	A-la-carte	Bundles			
			Enterprise Protection	SMB Protection	Unified Threat Protection	Advanced Threat Protection
Security Services	FortiGuard IPS Service	•	•	•	•	•
	FortiGuard Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•	•
	FortiGuard Web Security — URL and web content, Video and Secure DNS Filtering	•	•	•	•	
	FortiGuard Anti-Spam		•	•	•	
	FortiGuard IoT Detection Service	•	•			
	FortiGuard Industrial Security Service	•	•			
	FortiCloud AI-based Inline Sandbox Service [1]	•				
NOC Services	FortiGate Cloud (SMB Logging + Cloud Management)	•		•		
	FortiGuard Security Fabric Rating and Compliance Monitoring Service	•	•			
	FortiConverter Service	•	•			
	FortiGuard SD-WAN Underlay Bandwidth and Quality Monitoring Service	•				
SOC Services	FortiAnalyzer Cloud	•				
	FortiAnalyzer Cloud with SOCaaS	•				
Hardware and Software Support	FortiCare Essentials	•				
	FortiCare Premium	•	•	•	•	•
	FortiCare Elite	•				
Base Services	FortiGuard Application Control					
	FortiCloud ZTNA Inline CASB Service [1]					
	Internet Service (SaaS) DB Updates					
	GeoIP DB Updates		included with FortiCare Subscription			
	Device/OS Detection Signatures					
	Trusted Certificate DB Updates					
	DDNS (v4/v6) Service					

[1.] Available when running FortiOS 7.2

FortiGuard Bundles

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

FortiCare Elite

FortiCare Elite services offers enhanced service-level agreements (SLAs) and accelerated issue resolution. This advanced support offering provides access to a dedicated support team. Single-touch ticket handling by the expert technical team streamlines resolution. This option also provides Extended End-of-Engineering-Support (EoE's) of 18 months for added flexibility and access to the new FortiCare Elite Portal. This intuitive portal provides a single unified view of device and security health.

Fortinet CSR 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.

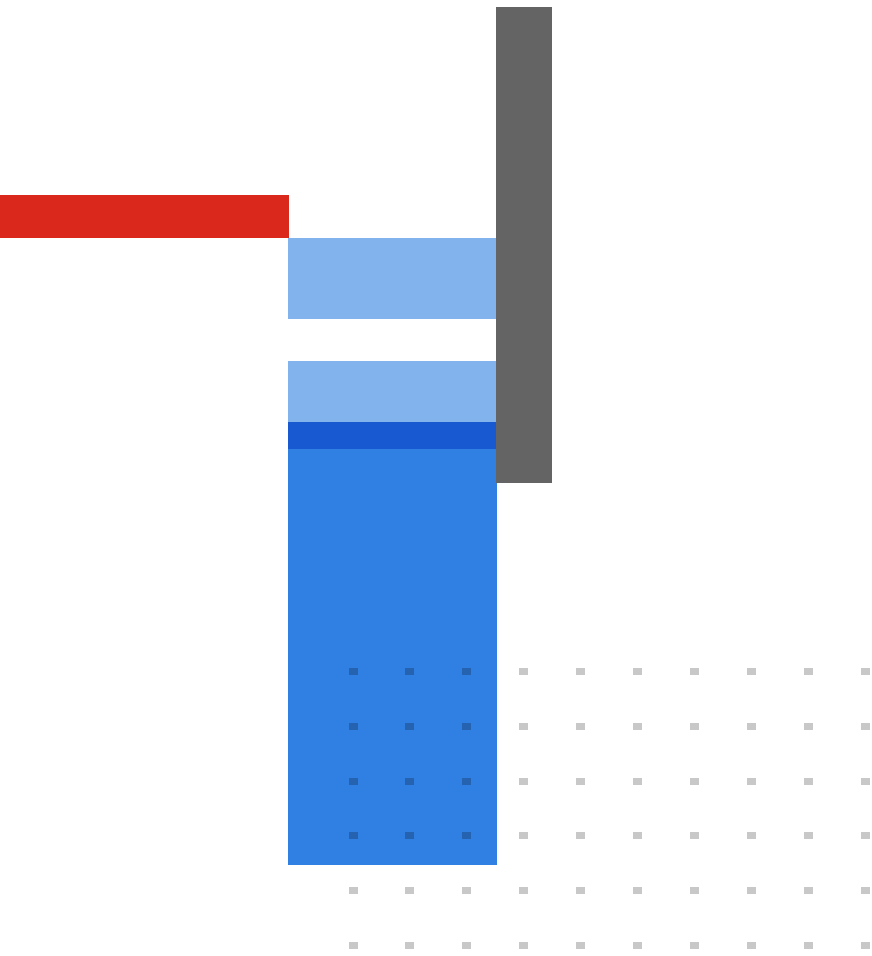# Ordering Information

Product	SKU	Description
FortiGate 40F	FG-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports).
FortiWiFi 40F	FWF-40F-[RC]	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), Wireless (802.11a/b/g/n/ac-W2).
FortiGate 40F-3G4G	FG-40F-3G4G	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports) with Embedded 3G/4G/LTE wireless wan module, external SMA WWAN antennas included.
FortiWiFi 40F-3G4G	FWF-40F-3G4G-[RC]	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports) with Embedded 3G/4G/LTE wireless wan module, Wireless (802.11a/b/g/n/ac-W2), external SMA WWAN and wireless antennas included.
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/FWF-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/FWF-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

FERTINET

www.fortinet.com

December 7, 2022

FGFWF-40F-DAT-R27-20221207