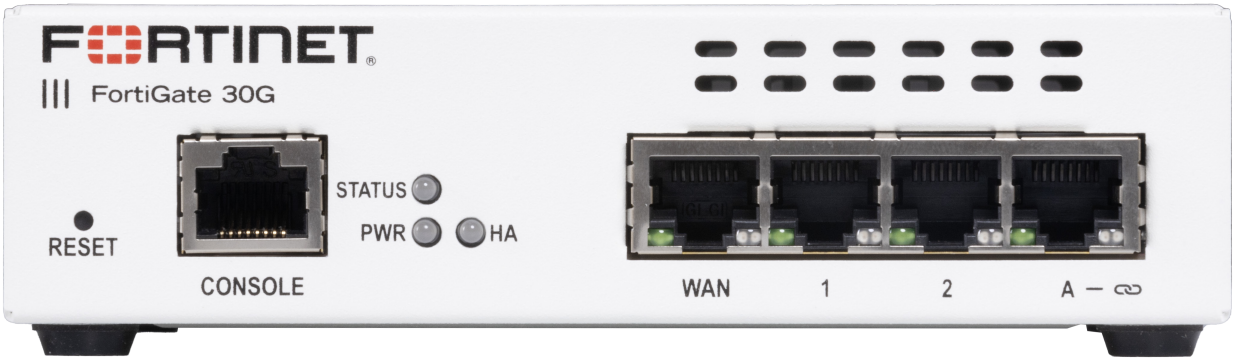
Data Sheet

FortiGate FortiWiFi 30G Series

FG-30G, FWF-30G



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 and SD-WAN

The FortiGate FortiWiFi 30G series integrates firewalling, SD-WAN and security in one appliance, ideal for building security-driven networks at distributed enterprise sites and transforming WAN architecture at any scale.

The FortiGate FortiWiFi 30G series is powered by the FortiOS operating system with the industry's first converged networking and security. This convergence enables businesses to efficiently secure today's dynamic digital infrastructures.

As a cornerstone of the Fortinet Security Fabric platform, the FortiGate Next Generation Firewall (NGFW) works seamlessly with FortiGuard AI-powered Security Services to deliver coordinated, automated, end-to-end threat protection across all use cases in real time.

The 30G family is built on the patented SD-WAN-based ASIC, delivering unmatched performance over traditional CPU with lower cost and power consumption. This application-specific design and embedded multi-core processor further accelerates the convergence of networking and security functions in the 30G family to optimize secure connection and user experience at branch locations.

IPS	NGFW	Threat Protection	Interfaces
800 Mbps	570 Mbps	500 Mbps	4x GE RJ45 ports (including 3x internal ports and 1x WAN port) | Wireless Variant

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.

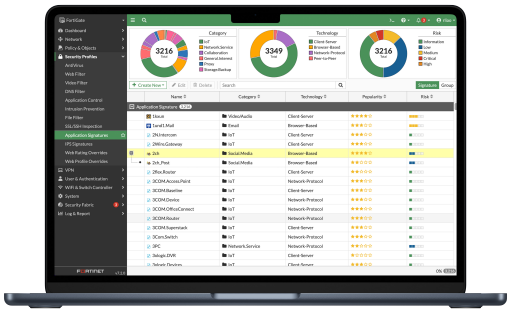
FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into organically built best-of-breed capabilities, unified operating system, and ultra-scalability. 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

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

SaaS and Data Security Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management, and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. The FortiGuard Data Loss Prevention Service provides advanced data protection by using real-time data classification and pattern matching to identify sensitive information. It offers comprehensive monitoring and control over data movement, ensuring that sensitive data is not inadvertently or maliciously transmitted outside the organization. Additionally, The FortiGuard Data Loss Prevention Service facilitates compliance with various regulatory requirements by automating the enforcement of data security policies and providing detailed reporting and audit trails.

Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

OT Security

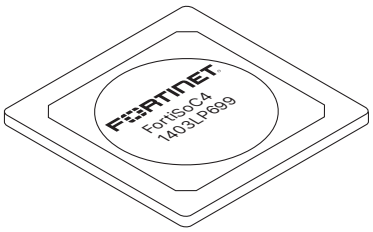
The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

Secure Any Edge at Any Scale

Powered by Security Processing Unit (SPU)

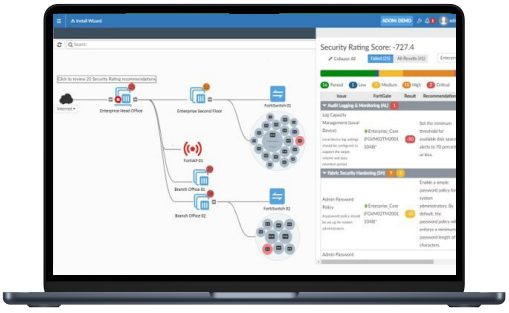
Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and 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



Intuitive view and clear insights into network security posture with FortiManager

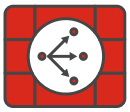
Centralized Network and Security Management at Scale

FortiManager, the centralized management solution from Fortinet, enables integrated management of the Fortinet security fabric, including devices like FortiGate, FortiSwitch, and FortiAP. It simplifies and automates the oversight of network and security functions across diverse environments, serving as the fundamental component for deploying Hybrid Mesh Firewalls.

Use Cases

Perimeter Protection

- Inspect and control incoming and outgoing traffic based on defined security policies
- FortiGuard AI-powered Security Services—natively integrated with your NGFW—secures your web, content, and devices, and proactively 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) with converged security and networking technologies provides accelerated performance, protection, and energy efficiency



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 applications identification which avoids delay in accessing applications and accelerates overlay performance regardless locations
- Enhances work-from-anywhere 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

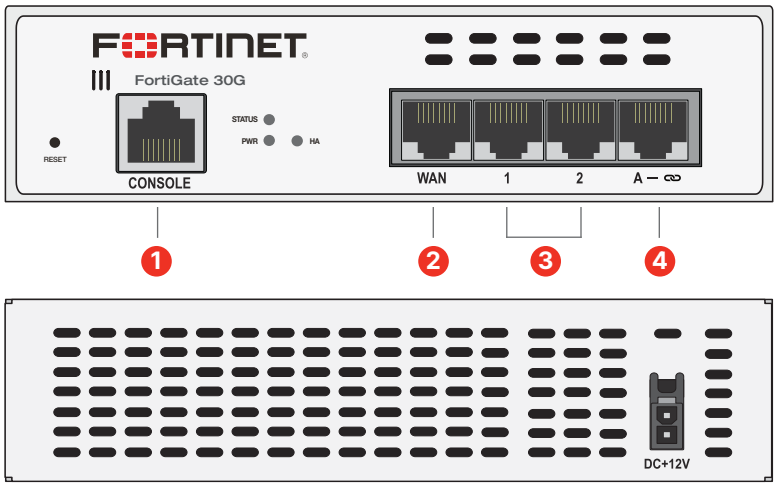
Secure Branch

- The Fortinet single Security Fabric platform enables FortiGate NGFWs to automatically discover and secure IoT devices for faster branch onboarding
- Fully integrated with FortiSwitch 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 that gives IT teams centralized visibility to simplify management across locations
- FortiGate HA support ensures continuous network protection and minimizes downtime in the event of hardware failures or network disruptions

Hardware

FortiGate FG-30G

SoC4 TPM DESKTOP GE

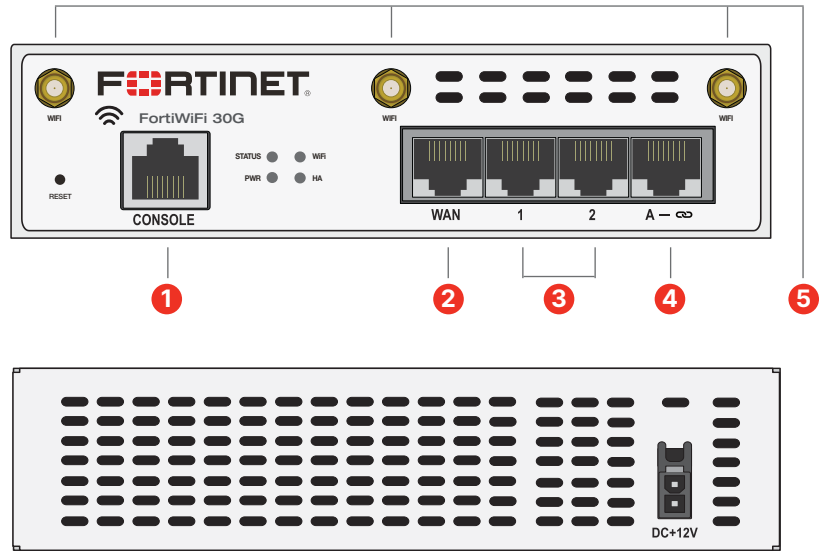


Interfaces

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

FortiWiFi FWF-30G

SoC4 TPM DESKTOP GE a/b/g/n/ac-W2/ax



Interfaces

1. 1 x Console Port
2. 1 x GE RJ45 WAN Port
3. 2 x GE RJ45 Ports
4. 1 x GE RJ45 FortiLink Port
5. 3 x WiFi Antenna Ports

Hardware Features

Superior Wireless Coverage

A built-in dual-band, dual-stream access point is integrated on the FortiWiFi 30G series which provides the industry's latest high-speed WiFi-6 (802.11ax) wireless access.

Trusted Platform Module (TPM)

The FortiGate FortiWiFi 30G series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.

Access Layer Security

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

Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight, yet highly reliable with a superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Specifications

	FORTIGATE 30G	FORTIWIFI 30G
Hardware Specifications		
Hardware Accelerated GE WAN Port	1	1
Hardware Accelerated GE RJ45 Ports	2	2
Hardware Accelerated GE RJ45 FortiLink Port (Default)	1	1
USB Ports	—	—
Console Port (RJ45)	1	1
Trusted Platform Module (TPM)	✓	✓
Bluetooth Low Energy (BLE)	—	—
Wireless Interface	—	Dual Radio (2.4 GHz/ 5 GHz), 802.11 a/b/g/n/ac/ax
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	800 Mbps	
NGFW Throughput [2, 4]	570 Mbps	
Threat Protection Throughput [2, 5]	500 Mbps	
System Performance		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	4/ 4/ 3.9 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	4/ 4/ 3.9 Gbps	
Firewall Latency (64 byte UDP packets)	2.87 µs	
Firewall Throughput (Packets Per Second)	5.85 Mpps	
Concurrent Sessions (TCP)	600 000	
New Sessions/Second (TCP)	30 000	
Firewall Policies	2000	
IPsec VPN Throughput (512 byte) [1]	3.5 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	200	
Client-to-Gateway IPsec VPN Tunnels	250	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	—	
SSL-VPN Throughput	—	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	400 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	260	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000	
Application Control Throughput (HTTP 64K) [2]	830 Mbps	
CAPWAP Throughput (HTTP 64K)	TBA Gbps	

	FORTIGATE 30G	FORTIWIFI 30G
Virtual Domains (Default/Maximum)	Not Supported	
Maximum Number of FortiSwitches Supported	8	
Maximum Number of FortiAPs (Total/Tunnel Mode)	16/8	
Maximum Number of FortiTokens	500	
High Availability Configurations	Active-Passive, Active-Active	
Dimensions		
Height x Width x Length (inches)	1.6 × 5.6 × 6.3	
Height x Width x Length (mm)	40.5 × 142 × 160	
Weight	1.3 lbs (0.6 kg)	1.5 lbs (0.7 kg)
Rack Mount Type	NA	
Wall Mountable	Optional	
Form Factor (supports EIA/ non-EIA standards)	Desktop	
Operating Environment and Certifications		
Power Rating	12VDC, 2A	
Power Source Powered by external DC power adapter	100-240V AC, 50/60 Hz	
Maximum Current	100V/0.11A, 240V/0.055A	110V/0.17A, 240V/0.085A
Power Consumption (Average/Maximum)	6.8 W / 8.2 W	11.3 W / 13.6 W
Heat Dissipation	28 BTU/hr	46 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	20% to 90% non-condensing	
Noise Level	N/A	
Operating Altitude	10 000 ft (3048 m)	
Compliance	FCC, IC, CE, UL/cUL, CB, VCCI, BSMI, RCM, UKCA	
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. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.

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 Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive lifecycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service variants, offers 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. Access the intuitive FortiCare Elite Portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

Ordering Information

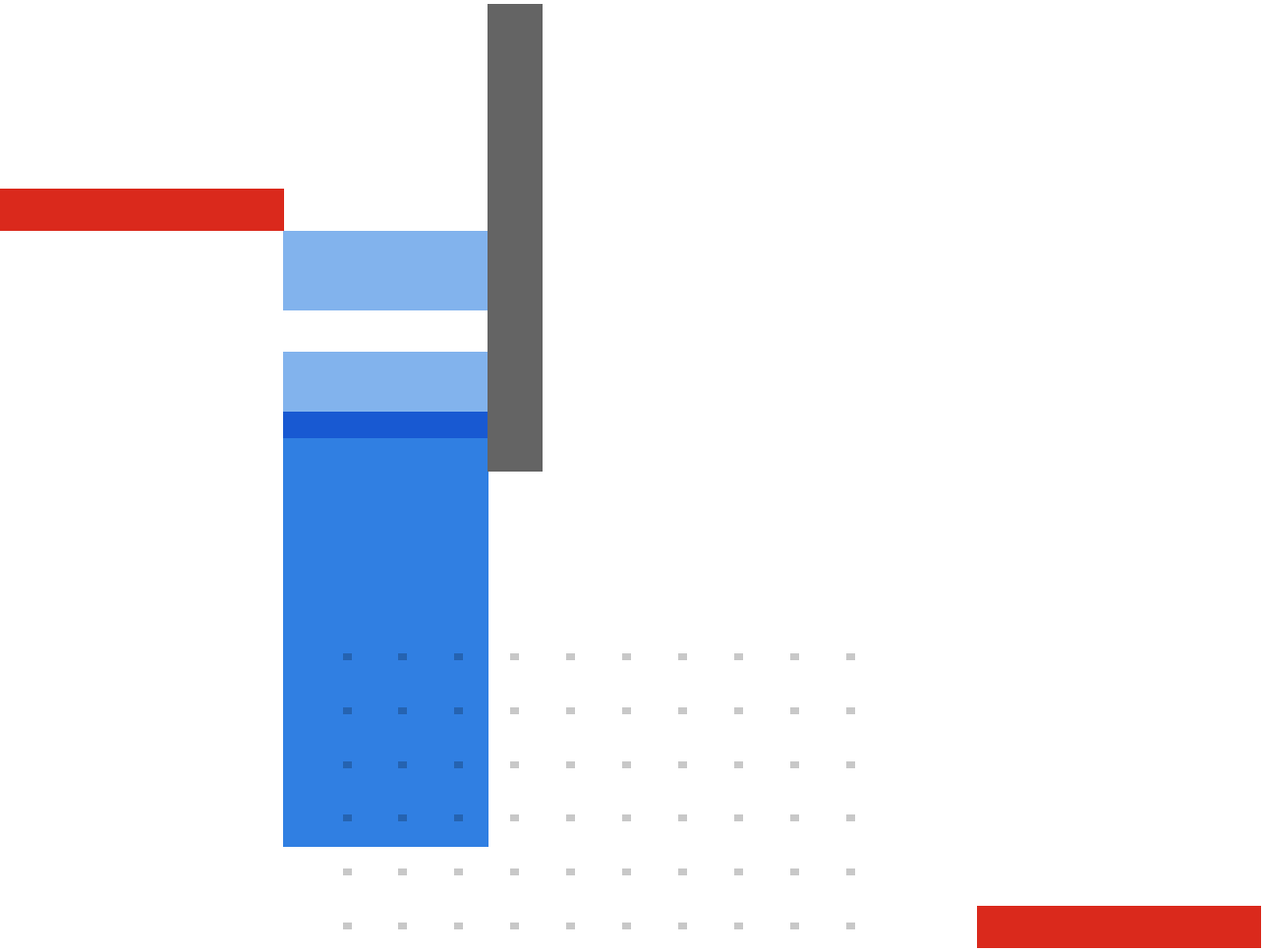
Product	SKU	Description
FortiGate 30G	FG-30G	4x GE RJ45 ports (including 3x Internal Ports, 1x WAN Port).
FortiWiFi 30G	FWF-30G	4x GE RJ45 ports (including 3x Internal Ports, 1x WAN Port), Wireless (802.11a/b/g/n/ac/ax).
Optional Accessories		
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-30G, FG/FWF-50G series, FG/FWF-60F series , and FG/FWF-80F series.
AC Power Adaptor	SP-FG-30G-PA-10(-XX)	Pack of 10 AC power adaptors for FG/FWF-30G, come with interchangeable power plugs. (XX=various countries code).

[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

August 23, 2024

FGFWF-30G-DAT-R01-20240823