FortiGate Rugged Firewalls

reddot winner 2024

CONTROL ENGINEERING 2024 PRODUCT OF THE YEAR

Highlights

Ruggedized Appliance with fanless design ensures reliable operations in harsh conditions

Unparalleled Performance enabled by Fortinet's patented secure processors and FortiOS operating system

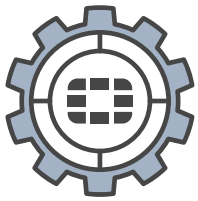
Enterprise-grade Protection with consolidated FortiGuard AI-powered Security Services

Built-in SD-WAN supports reliable connectivity with lower costs and better user experience

Simplified Management enables faster deployment, comprehensive monitoring, security automation, and easier management

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

Next-generation firewalls (NGFW) for building security-driven networks without impacting network performance.



Security Solutions for Mission Critical Industrial Environments

FortiGate Rugged Series next-generation firewalls (NGFW) are best for building security-driven networks without impacting network performance.

These NGFWs are built to withstand harsh environmental conditions commonly found in industrial networks and operational technology (OT).

Unlike traditional security solutions made for office and enterprise networks, the FortiGate Rugged Series is industrially rugged and offer all-in-one security appliances with advanced threat protection capabilities for securing critical industrial networks against cyber threats.

Overview

Model	IPS	NGFW	ATP	Interfaces
FGR-50G-5G	2.25 Gbps	1.25 Gbps	1.1 Gbps	• 6 GE RJ45 ports • 2 SFP slots • Digital I/O module • Single 5G modem and GPS • Dual SIM (active/passive) • Redundant 12V-54V DC inputs
FGR-60F **FGR-60F-3G4G**	950 Mbps	550 Mbps	500 Mbps	• 4 GE RJ45 ports • 2 shared GE RJ45 ports/SFP slots • 1 bypass pair • Variant with single 3G/4G LTE modem and GPS • Dual SIM (active/passive) • Redundant 12V-125V DC inputs
FGR-70F **FGR-70F-3G4G**	975 Mbps	950 Mbps	580 Mbps	• 6 GE RJ45 ports • 2 SFP slots • 1 bypass pair • MicroSD card slot • Digital I/O module • Variant with single 3G/4G LTE modem and GPS • Dual SIM (active/passive) • Redundant 12V-125V DC inputs
FGR-70G-5G-DUAL	2.5 Gbps	1.5 Gbps	1.3 Gbps	• 6 GE RJ45 ports • 2 SFP slots • 1 bypass pair • MicroSD card slot • Digital I/O module • Dual 5G modems and GPS • Dual SIM (active/active) • Redundant 12V-125V DC inputs

Available in:

Rugged Appliance

FortiOS Everywhere

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

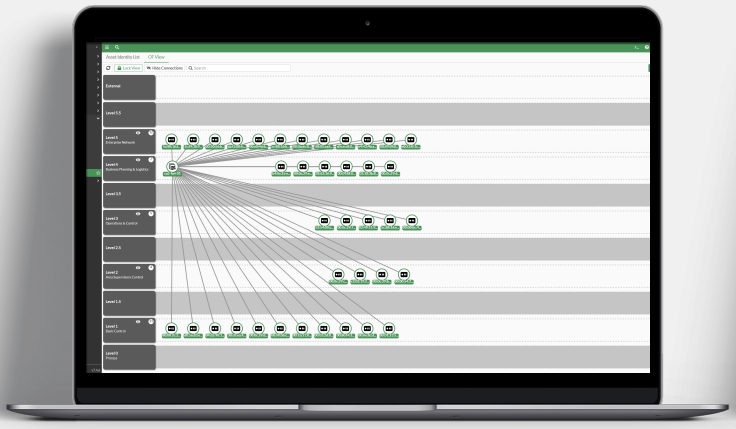
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

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.

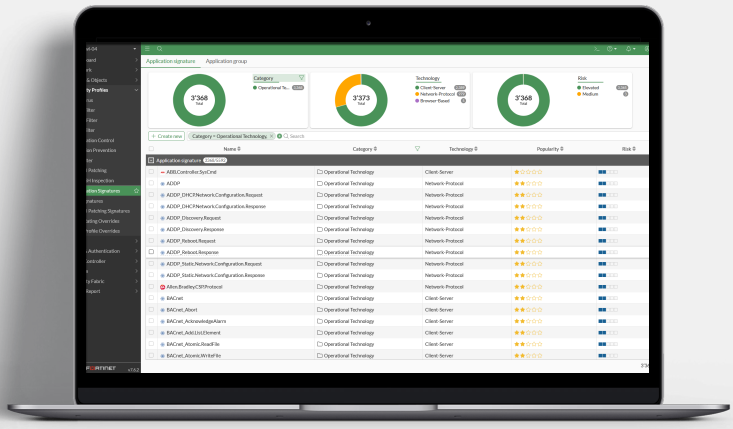
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more. It provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

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:

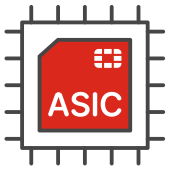
- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations



OT focused dashboard for assets and analytics



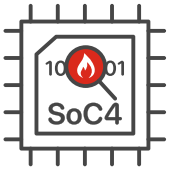
Visibility and control for OT applications and protocols

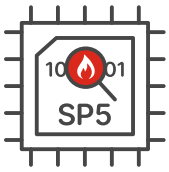


Secure Any Edge at Any Scale

Powered by The Only Purpose-Built 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.

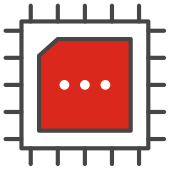




ASIC Advantage

Secure SD-WAN ASIC SOC4 and SP5

- 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

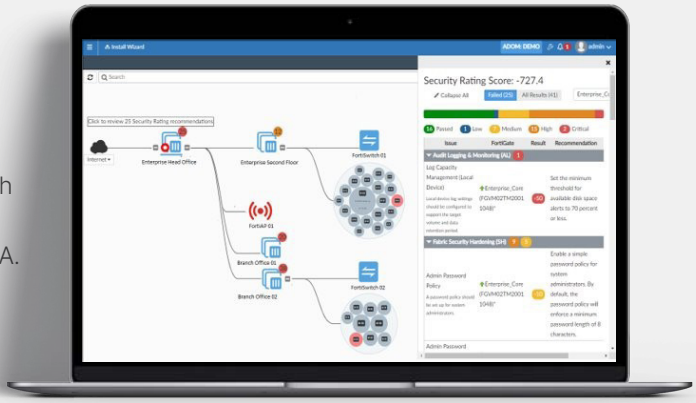


Trusted Platform Module (TPM)

The FortiGate Rugged 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.

Centralized Network and Security Management at Scale

FortiManager is a FortiAI-powered centralized management solution for Fortinet's Security Fabric in hybrid environments. It seamlessly integrates with FortiGate, FortiGate VM, cloud security, SD-WAN, SD-Branch, FortiSASE, and ZTNA. FortiManager simplifies and automates the management of network and security functions, leveraging GenAI technology in FortiAI to enhance Day 0-1 configuration, provisioning, and Day N troubleshooting and maintenance. This enables the full potential of Fortinet's Security Fabric, significantly improving operational efficiency.

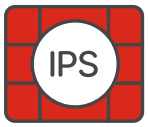


Intuitive view and clear insights into network security posture with FortiManager

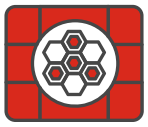
Use Cases

Industrial Security

- Implement industrial-grade security across the industrial networks with industry certified next-generation firewall appliances
- Secure industrial networks with deep packet inspection (DPI) for 80+ OT applications and protocols supporting up to payload level visibility and control

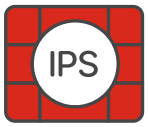


- Apply virtual patching or vulnerability shielding with OT-centric IPS (intrusion prevention system) and minimize risks against security threats that have potential to exploit known or unknown vulnerabilities



Network Segmentation and Microsegmentation

- Network segmentation implements the concept of security zones and conduits and prevent unauthorized access to critical OT assets, the firewall acts as a conduit between different zones and offers secure pathway for communication



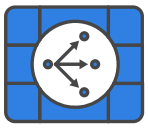
- Network segmentation limits the impact of any security incidents that occur within a specific zone and supports North and South network traffic monitoring and threat protection
- Network microsegmentation further segments the security zones based on different security requirements and supports East and West network traffic monitoring and deep packet inspection preventing lateral movement attacks

Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your FortiGate Rugged NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks

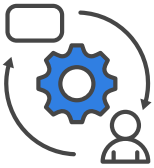
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection

Use Cases



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
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing



Universal ZTNA

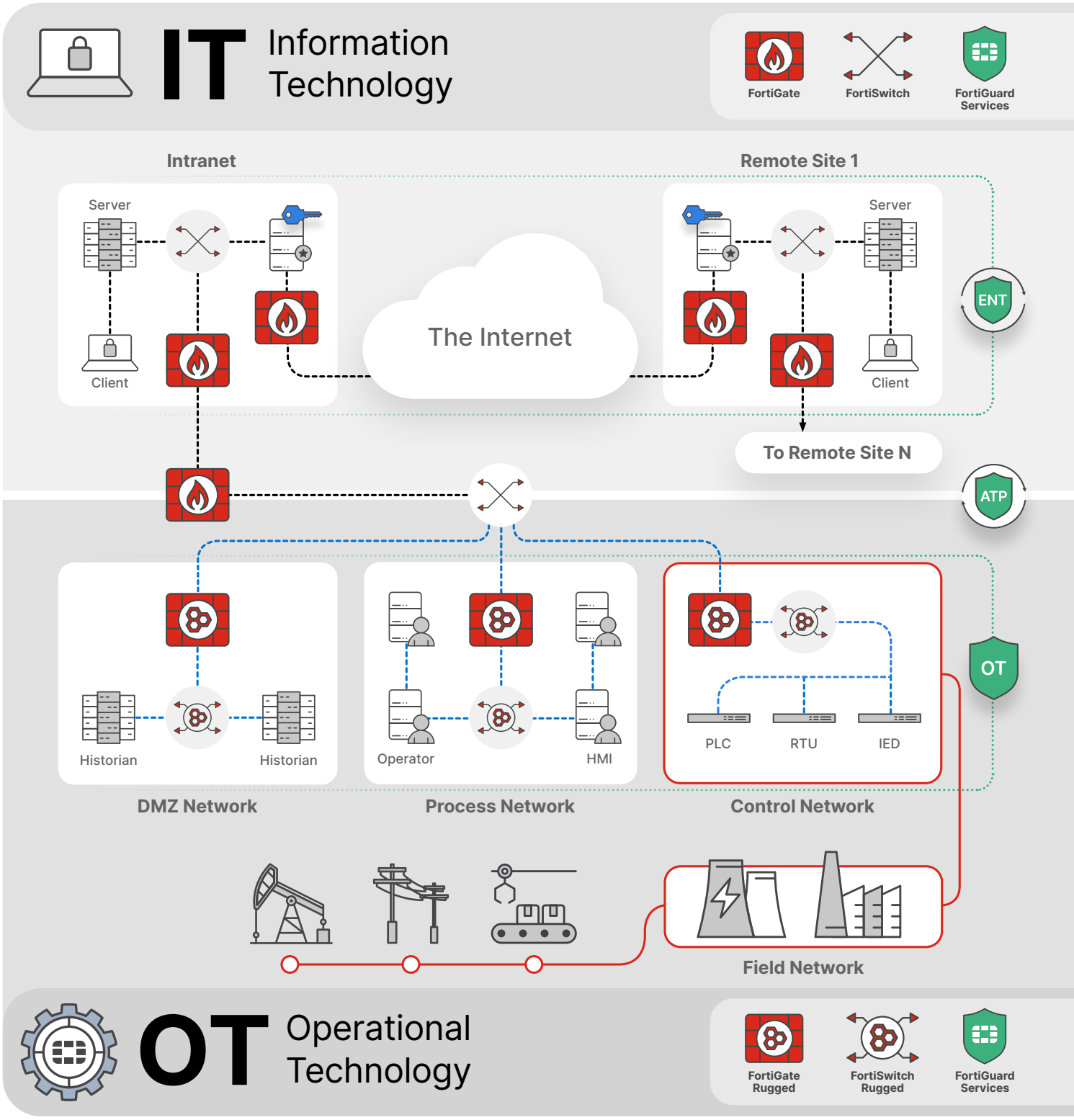
- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access—every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

Access Layer Security

- The Fortinet single Security Fabric platform enables FortiGate NGFWs to automatically discover and secure IoT and IIoT devices for faster branch onboarding
- Fully integrated with FortiSwitch ethernet switches and FortiAP access points, FortiGate easily extends security to LAN, WAN, and WLAN at branch offices or remote sites for unified protection and reliable connectivity
- FortiGate and Fortinet products work seamlessly with FortiManager that gives IT/OT teams centralized visibility to simplify management across locations
- 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.

Use Cases

Typical Deployment of FortiGate Firewalls in IT/OT Networks



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 service 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. FortiGuard DLP 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, FortiGuard DLP 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.

Visit FortiGuard OT Security Service page to view the latest list of OT applications and protocols included in the FortiGuard OT Security Service.

Product Range

FortiGate Rugged Firewalls

FGR-50G-5G

FGR-60F-3G4G

FGR-70F-3G4G

FGR-70G-5G-DUAL

FGR-60F

FGR-70F

Specifications

	FGR-70F	FGR-70F-3G4G	FGR-70G-5G-DUAL
Interfaces and Modules			
GE RJ45 Interfaces	6	6	6
Bypass GE RJ45 Port Pair	PORT3 and PORT4	PORT3 and PORT4	PORT1 and PORT2
Dedicated GE SFP Slots	2	2	2
Serial Interface (RJ45)	1	1	1
USB 2.0 (Client / Server)	1	1	1
Console Port (RJ45)	1	1	1
Cellular Modem	—	3G / 4G LTE, GPS	Dual 5G, GPS
Bluetooth Low Energy (BLE)	✓	✓	✓
Transceivers Included	—	—	—
Processor	FortiSoC4	FortiSoC4	FortiSP5
Trusted Platform Module (TPM)	✓	✓	✓
Digital I/O Module (DIO)	✓	✓	✓
MicroSD Card Slot	✓	✓	✓
System Performance and Capacity*			
IPv4 Firewall Throughput (1518/512/64 byte UDP packets)	8/8/8 Gbps	8/8/8 Gbps	8/8/8 Gbps
Firewall Latency (64 byte, UDP)	6.71 µs	6.71 µs	5.82 µs
Firewall Throughput (Packets Per Second)	12 Mpps	12 Mpps	12 Mpps
Concurrent Sessions (TCP)	1 M	1 M	1.4 M
New Sessions/Second (TCP)	35 000	35 000	85 000
Firewall Policies	5000	5000	5000
IPsec VPN Throughput (512 byte) [1]	6.5 Gbps	6.5 Gbps	7.1 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200	200	200
Client-to-Gateway IPsec VPN Tunnels	500	500	500
SSL-VPN Throughput[6]	450 Mbps	450 Mbps	—
Concurrent SSL-VPN Users[6] **(Recommended Maximum)**	100	100	—
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	500 Mbps	500 Mbps	1.4 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	380	380	715
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	90 000	90 000	1.4 M
Application Control Throughput (HTTP 64K)	1.1 Gbps	1.1 Gbps	3.6 Gbps
Virtual Domains (Default/Maximum)	10 / 10	10 / 10	10 / 10
Maximum Number of FortiAPs (Total/Tunnel)	64 / 32	64 / 32	96 / 48
Maximum Number of FortiTokens	500	500	500
Maximum Number of FortiSwitches	24	24	24
High Availability Configurations	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering

* Performance metrics are provisional and subject to change.

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 feature is not supported starting with FortiOS v7.6.0. It is recommended to use FortiOS v7.2.x LTS release to access these features on the affected models.

Specifications

	FGR-70F	FGR-70F-3G4G	FGR-70G-5G-DUAL
System Performance — Enterprise Traffic Mix			
IPS Throughput [2]	975 Mbps	975 Mbps	2.5 Gbps
NGFW Throughput [2, 4]	950 Mbps	950 Mbps	1.5 Gbps
Threat Protection Throughput [2, 5]	580 Mbps	580 Mbps	1.3 Gbps
Dimensions and Power			
Height x Width x Length (inches)	4.8 × 3.2 × 4.4	4.8 × 3.2 × 4.4	5.47 × 4.1 × 4.8
Height x Width x Length (mm)	122 × 80.5 × 111	122 × 80.5 × 111	139 × 104 × 122
Weight	2.87 lbs (1.3 kg)	2.87 lbs (1.3 kg)	4.63 lbs (2.1 kg)
Form Factor	DIN-rail	DIN-rail	DIN-rail
Antenna (Height x Width)	—	205 mm x 25 mm	205 mm x 25 mm
IP Rating	IP40	IP40	IP40
Power Supply	Redundant dual inputs, 2 pins per terminal block, supports negative (+12V to +125V DC) and positive (-12V to -125V DC) ground power sources, DC cables are not included.	Redundant dual inputs, 2 pins per terminal block, supports negative (+12V to +125V DC) and positive (-12V to -125V DC) ground power sources, DC cables are not included.	Redundant dual inputs, 2 pins per terminal block, supports negative (+12V to +125V DC) and positive (-12V to -125V DC) ground power sources, DC cables are not included.
Power Consumption (Average / Maximum)	16 W /18 W	18.3 W /19.9 W	18.3 W /19.9 W
Maximum Current	12V DC / 1.5A	12V DC / 1.67A	12V DC / 1.67A
Heat Dissipation	62 BTU/h	68 BTU/h	68 BTU/h
Operating Environment			
Operating Temperature	-40°F to 167°F (-40°C to 75°C)	-40°F to 167°F (-40°C to 75°C)	-40°F to 167°F (-40°C to 75°C)
Storage Temperature	-40°F to 185°F (-40°C to 85°C)	-40°F to 185°F (-40°C to 85°C)	-40°F to 185°F (-40°C to 85°C)
Humidity	5% to 95% non-condensing	5% to 95% non-condensing	5% to 95% non-condensing
Operating Altitude	Up to 10 000 ft (3048 m)	Up to 10 000 ft (3048 m)	Up to 10 000 ft (3048 m)

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 feature is not supported starting with FortiOS v7.6.0. It is recommended to use FortiOS v7.2.x LTS release to access these features on the affected models.

Specifications

	FGR-70F	FGR-70F-3G4G	FGR-70G-5G-DUAL
Industry Compliance and Certifications			
Electric Power Industry	IEC 61850-3 and IEEE 1613 Certified	IEC 61850-3 and IEEE 1613 Certified	IEC 61850-3 and IEEE 1613 Certified
EMC	EN 55032:2015 + A11:2020, Class A EN 55035:2017 + A11:2020 ETSI EN 301 489-1 V2.2.3 (2019-11) ETSI EN 301 489-17 V3.2.4 (2020-09)	EN 55032:2015 + A11:2020, Class A EN 55035:2017 + A11:2020 ETSI EN 301 489-1 V2.2.3 (2019-11) ETSI EN 301 489-17 V3.2.4 (2020-09) ETSI EN 301 489-19 V2.1.1 (2019-04) ETSI EN 301 489-52 V1.2.1 (2021-11)	EN 55032:2015 + A1:2020, Class A EN 55035:2017 + A11:2020 ETSI EN 301 489-1 V2.2.3 (2019-11) ETSI EN 301 489-17 V3.2.4 (2020-09) ETSI EN 301 489-19 V2.1.1 (2019-04) ETSI EN 301 489-52 V1.2.1 (2021-11)
Health and Safety	IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 + A11:2017 IEC 62368-1: 2018, 3rd Ed. EN IEC 62368-1:2020 + A11:2020	IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 + A11:2017 IEC 62368-1: 2018, 3rd Ed. EN IEC 62368-1:2020 + A11:2020	IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 IEC 62368-1:2018, 3rd Ed. EN IEC 62368-1:2020
Regulatory Compliance	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/cUL, CB USGv6/IPv6
RF	ETSI EN 300 328 V2.2.2 (2019-07) EN IEC 62311:2020 EN 50665:2017 FCC Part 15 Subpart C 15.247 FCC 47 CFR Part 2.1091 ISED RSS-247 Issue 2 RSS-102 Issue 5	EN 301 908-1 V15.1.1 (2021-09) EN 301 908-2 V13.1.1 (2020-06) EN 301 908-13 V13.1.1 (2019-11) ETSI EN 300 328 V2.2.2 (2019-07) EN 303 413 V1.2.1 (2021-04) EN IEC 62311:2020 EN 50665:2017 FCC Part 15 Subpart C 15.247 FCC 47 CFR Part 2.1091 ISED RSS-247 Issue 2 RSS-102 Issue 5	EN 301 908-1 V15.2.1 (2023-01) EN 301 908-2 V13.1.1 (2020-06) EN 301 908-13 V13.2.1 (2022-02) Draft EN 301 908-25 V15.1.1 EN 300 328 V2.2.2 (2019-07) EN 303 413 V1.2.1 (2021-04) EN IEC 62311:2020 EN 50665:2017 FCC Part 15 Subpart C 15.247 FCC 47 CFR Part 2.1091 ISED RSS-247 Issue 3 RSS-102 Issue 6
RoHS	EN IEC 63000:2018 EN 50581:2012	EN IEC 63000:2018 EN 50581:2012	EN IEC 63000:2018 EN 50581:2012
Rolling Stock Industry	EN 50155:2021 EN 50121-1:2017 EN 50121-3-2:2016 + A1:2019 EN 50121-4:2016 + A1:2019 EMC, Environmental, Shock and Vibration Certified	EN 50155:2021 EN 50121-1:2017 EN 50121-3-2:2016 + A1:2019 EN 50121-4:2016 + A1:2019 EMC, Environmental, Shock and Vibration Certified	EN 50155:2021 EN 50121-1:2017 EN 50121-3-2:2016 + A1:2019 EN 50121-4:2016 + A1:2019 EMC, Environmental, Shock and Vibration Certified

	FGR-70F-3G4G	FGR-70G-5G-DUAL
Cellular Wireless		
Maximum Tx Power	20 dBm	23 dBm (Power Class 3), 26 dBm (Power Class 2 in B41/n41)
Regions	All Regions	All Regions
Modem Model	Sierra Wireless EM7565 (2 SIM Slots, Active/Passive)	Telit Cinterion FN990A28-HP (2 SIM Slots, Active/Active)
5G Bands	—	n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n29 (SDL), n30, n38, n40, n41, n48, n66, n71, n75 (SDL), n76 (SDL), n77, n78, n79 (PC1.5 support on n41, n77, n78, n79 bands)
LTE	B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B18, B19, B20, B26, B28, B29, B30, B32, B41, B42, B43, B46, B48, B66	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29 (SDL), B30, B32 (SDL), B34, B38, B39, B40, B41, B42, B43, B46, B48, B66, B71
UMTS/HSPA+	B1, B2, B3, B4, B5, B6, B8, B9, B29	B1, B2, B4, B5, B6, B8, B19
WCDMA	—	B1, B2, B4, B5 (B6, B19), B8 (for EU and APAC regions only)
CDMA 1xRTT/EV-DO Rev A	—	—
GSM/GPRS/EDGE	—	—
Module Certifications	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC, IC, RED, NCC, JATE/TELEC, KC, NCC+, RCM, GCF, PTCRB, AT&T, FirstNet, KDDI, KT, Telstra, T-Mobile US, Verizon
Carrier Certifications	—	PTCRB, AT&T, Verizon, T-Mobile
Diversity	✓	✓
MIMO	✓	✓
GNSS Bias	✓	✓

Specifications

	FGR-60F	FGR-60F-3G4G
Interfaces and Modules		
GE RJ45 Interfaces	4	4
Bypass GE RJ45 Port Pair	PORT4 and WAN1	PORT4 and WAN1
GE RJ45/SFP Shared Media Pairs	2	2
Serial Interface	1 DB9	1 DB9
USB (Client / Server)	1	1
RJ45 Console Port	1	1
Cellular Modem	—	3G / 4G LTE, GPS
Bluetooth Low Energy (BLE)	—	—
Transceivers Included	—	—
Processor	FortiSoC4	FortiSoC4
Trusted Platform Module (TPM)	✓	✓
Digital I/O Module (DIO)	—	—
MicroSD Card Slot	—	—
System Performance and Capacity		
IPv4 Firewall Throughput (1518/ 512 / 64 byte UDP packets)	6/6/5.95 Gbps	6/6/5.95 Gbps
Firewall Latency (64 byte, UDP)	3.10 µs	3.10 µs
Firewall Throughput (Packets Per Second)	8.9 Mpps	8.9 Mpps
Concurrent Sessions (TCP)	600 000	600 000
New Sessions/Second (TCP)	19 000	19 000
Firewall Policies	5000	5000
IPsec VPN Throughput (512 byte) [1]	3.5 Gbps	3.5 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200	200
Client-to-Gateway IPsec VPN Tunnels	500	500
SSL-VPN Throughput[6]	400 Mbps	400 Mbps
Concurrent SSL-VPN Users[6] (Recommended Maximum)	100	100
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	460 Mbps	460 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	300	300
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	70 000	70 000
Application Control Throughput (HTTP 64K)	1.3 Gbps	1.3 Gbps
Virtual Domains (Default / Maximum)	10 / 10	10 / 10
Maximum Number of FortiAPs (Total / Tunnel)	30 / 10	30 / 10
Maximum Number of FortiTokens	500	500
Maximum Number of FortiSwitches	24	24
High Availability Configurations	Active-Active, Active-Passive, Clustering	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 feature is not supported starting with FortiOS v7.6.0. It is recommended to use FortiOS v7.2.x LTS release to access these features on the affected models.

Specifications

	FGR-60F	FGR-60F-3G4G
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	950 Mbps	950 Mbps
NGFW Throughput [2, 4]	550 Mbps	550 Mbps
Threat Protection Throughput [2, 5]	500 Mbps	500 Mbps
Dimensions and Power		
Height x Width x Length (inches)	1.68 × 8.50 × 6.70	1.68 × 8.50 × 6.70
Height x Width x Length (mm)	42.7 × 216 × 170	42.7 × 216 × 170
Weight	3.85 lbs (1.75 kg)	4.06 lbs (1.84 kg)
Form Factor	Desktop/ DIN-rail/ Wall Mount	Desktop/ DIN-rail/ Wall Mount
Antenna (Height x Width)		205 mm x 25 mm
IP Rating	IP20	IP20
Power Supply	Redundant dual inputs, 2 pins per terminal block, supports negative (+12V to +125V DC) and positive ground (-12V to -125V DC) power sources, DC cables are not included.	Redundant dual inputs, 2 pins per terminal block, supports negative (+12V to +125V DC) and positive ground (-12V to -125V DC) power sources, DC cables are not included.
Power Consumption (Average / Maximum)	15 W / 21 W	16 W / 24 W
Maximum Current	12V DC / 2A	12V DC / 2A
Heat Dissipation	72 BTU/h	82 BTU/h
Operating Environment		
Operating Temperature	-40°F to 167°F (-40°C to 75°C)	-40°F to 167°F (-40°C to 75°C)
Storage Temperature	-40°F to 185°F (-40°C to 85°C)	-40°F to 185°F (-40°C to 85°C)
Humidity	5% to 95% non-condensing	5% to 95% non-condensing
Operating Altitude	Up to 10 000 ft (3048 m)	Up to 10 000 ft (3048 m)

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 feature is not supported starting with FortiOS v7.6.0. It is recommended to use FortiOS v7.2.x LTS release to access these features on the affected models.

Specifications

	FGR-60F	FGR-60F-3G4G
Industry Compliance and Certifications		
Electric Power Industry	IEC 61850-3 and IEEE 1613 Certified	IEC 61850-3 and IEEE 1613 Certified
EMC	EN 55032:2015 + A11:2020, Class A EN 55035:2017 + A11:2020 EN IEC 61000-6-4:2019 IEC 61000-4-9 IEC 61000-4-10	EN 55032:2015 + A11:2020, Class A EN 55035:2017 + A11:2020 EN IEC 61000-6-4:2019 IEC 61000-4-9 IEC 61000-4-10 ETSI EN 301 489-1 V2.2.3 (2019-11) ETSI EN 301 489-19 V2.2.1 (2022-09) ETSI EN 301 489-52 V1.2.1 (2021-11)
Health and Safety	IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 + A11:2017 IEC 62368-1: 2018, 3rd Ed. EN IEC 62368-1:2020 + A11:2020	IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 + A11:2017 IEC 62368-1: 2018, 3rd Ed. EN IEC 62368-1:2020 + A11:2020
Maritime Industry	IEC 60945:2002 4th Ed. DNV GL Type Approved (Tested with a rackmount)	IEC 60945:2002 4th Ed. DNV GL Type Approved (Tested with a rackmount)
Regulatory Compliance	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/cUL, CB
RF		EN 301 908-1 V15.1.1 (2021-09) EN 301 908-2 V13.1.1 (2020-06) EN 301 908-13 V13.1.1 (2019-11) EN 303 413 V1.2.1 (2021-04) EN 62311:2008 EN 50665:2017 FCC 47 CFR Part 2.1091 RSS-102 Issue 5
RoHS	EN IEC 63000:2018 EN 50581:2012	EN IEC 63000:2018 EN 50581:2012
Rolling Stock Industry	EMC, Shock and Vibration Compliant EN 50121-1:2017 EMC EN 50121-4:2016 EMC IEC 60068-2-27:2008 Shock IEC 60068-2-6:2007 Vibration	EMC Compliant EN 50121-1:2017 EMC EN 50121-4:2016 EMC
Cellular Wireless		
Maximum Tx Power	—	20 dBm
Regions	—	All Regions
Modem Model	—	Sierra Wireless EM7565 (2 SIM Slots, Active/Passive)
LTE	—	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+	—	B1, B2, B3, B4, B5, B6, B8, B9, B29
WCDMA	—	—
CDMA 1xRTT/EV-DO Rev A	—	—
GSM/GPRS/EDGE	—	—
Module Certifications	—	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB
Diversity	—	✓
MIMO	—	✓
GNSS Bias	—	✓

Specifications

	FGR-50G-5G
Interfaces and Modules	
GE RJ45 Interfaces	6
Bypass GE RJ45 Port Pair	—
Dedicated GE SFP Slots	2
Serial Interface (RJ45)	1
USB 2.0 (Client / Server)	1
Console Port (RJ45)	1
Cellular Modem	5G, GPS
Bluetooth Low Energy (BLE)	✓
Transceivers Included	—
Processor	FortiSP5
Trusted Platform Module (TPM)	✓
Digital I/O Module (DIO)	✓
MicroSD Card Slot	—
System Performance and Capacity	
IPv4 Firewall Throughput (1518/ 512 / 64 byte UDP packets)	6/6/6 Gbps
Firewall Latency (64 byte, UDP)	2.43 µs
Firewall Throughput (Packets Per Second)	9 Mpps
Concurrent Sessions (TCP)	700 000
New Sessions/Second (TCP)	85 000
Firewall Policies	2000
IPsec VPN Throughput (512 byte) [1]	5.3 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200
Client-to-Gateway IPsec VPN Tunnels	250
SSL-VPN Throughput[6]	N/A
Concurrent SSL-VPN Users[6] (Recommended Maximum)	N/A
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	1.3 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	699
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	74 000
Application Control Throughput (HTTP 64K)	3 Gbps
Virtual Domains (Default / Maximum)	5 / 5
Maximum Number of FortiAPs (Total / Tunnel)	16 / 8
Maximum Number of FortiTokens	500
Maximum Number of FortiSwitches	8
High Availability Configurations	Active-Active, Active-Passive, Clustering

	FGR-50G-5G
System Performance — Enterprise Traffic Mix	
IPS Throughput [2]	2.25 Gbps
NGFW Throughput [2, 4]	1.25 Gbps
Threat Protection Throughput [2, 5]	1.1 Gbps
Dimensions and Power	
Height x Width x Length (inches)	5.47 × 4.80 × 3.52
Height x Width x Length (mm)	139 × 122 × 89.5
Weight	3.97 lbs (1.8 kg)
Form Factor	DIN-rail
Antenna (Height x Width)	205 mm x 25 mm
IP Rating	IP40
Power Supply	Redundant dual inputs, 2 pins per terminal block, supports negative (+12V to +54V DC) and positive (-12V to -54V DC) ground power sources, DC cables are not included.
Power Consumption (Average / Maximum)	16 W / 24 W
Maximum Current	12V DC / 2A
Heat Dissipation	82 BTU/h
Operating Environment	
Operating Temperature	-40°F to 167°F (-40°C to 75°C)
Storage Temperature	-40°F to 185°F (-40°C to 85°C)
Humidity	5% to 95% non-condensing
Operating Altitude	Up to 10 000 ft (3048 m)

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 v7.6.0 and above, for models with 2GB RAM.

Specifications

	FGR-50G-5G
Industry Compliance and Certifications	
Electric Power Industry	IEC 61850-3 and IEEE 1613 Certified
EMC	EN 55032:2015 + A1:2020, Class A EN 55035:2017 + A11:2020 ETSI EN 301 489-1 V2.2.3 (2019-11) ETSI EN 301 489-17 V3.2.4 (2020-09) ETSI EN 301 489-19 V2.1.1 (2019-04) ETSI EN 301 489-52 V1.2.1 (2021-11)
Health and Safety	IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 IEC 62368-1:2018, 3rd Ed. EN IEC 62368-1:2020
Regulatory Compliance	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/cUL, CB, USGv6/IPv6
RF	EN 301 908-1 V15.2.1 (2023-01) EN 301 908-2 V13.1.1 (2020-06) EN 301 908-13 V13.2.1 (2022-02) Draft EN 301 908-25 V15.1.1 EN 300 328 V2.2.2 (2019-07) EN 303 413 V1.2.1 (2021-04) EN IEC 62311:2020 EN 50665:2017 FCC Part 15 Subpart C 15.247 FCC 47 CFR Part 2.1091 ISED RSS-247 Issue 3 RSS-102 Issue 6
RoHS	EN IEC 63000:2018, EN 50581:2012
Rolling Stock Industry	EN 50155:2021 EN 50121-1:2017 EN 50121-3-2:2016 + A1:2019 EN 50121-4:2016 + A1:2019 EMC, Environmental, Shock and Vibration Certified
Cellular Wireless	
Maximum Tx Power	23 dBm (Power Class 3), 26 dBm (Power Class 2 in B41/n41)
Regions	All Regions
Modem Model	Telit Cinterion FN990A28-HP (2 SIM Slots, Active/Passive)
5G Bands	n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n29 (SDL), n30, n38, n40, n41, n48, n66, n71, n75 (SDL), n76 (SDL), n77, n78, n79 (PC1.5 support on n41, n77, n78, n79 bands)
LTE	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29 (SDL), B30, B32 (SDL), B34, B38, B39, B40, B41, B42, B43, B46, B48, B66, B71
UMTS/HSPA+	B1, B2, B4, B5, B6, B8, B19
WCDMA	B1, B2, B4, B5 (B6, B19), B8 (for EU and APAC regions only)
CDMA 1xRTT/EV-DO Rev A	—
GSM/GPRS/EDGE	—
Module Certifications	FCC, IC, RED, NCC, JATE/TELEC, KC, NCC+, RCM, GCF, PTCRB, AT&T, FirstNet, KDDI, KT, Telstra, T-Mobile US, Verizon
Carrier Certifications	PTCRB, AT&T
Diversity	✓
MIMO	✓
GNSS Bias	✓

Ordering Information

Product	SKU	Description
FortiGate Rugged 50G-5G	FGR-50G-5G	Ruggedized, indoor, IP40, 4x GE RJ45 ports, 2x GE RJ45 WAN ports, 2x SFP slots, 1x RJ45 serial port (data), 1x RJ45 serial port (console), 1x USB port, 1x embedded 5G wireless WAN module (includes, 2 SIM slots - Active/Passive, 4x external SMA WWAN antennas), Passive GPS (includes 1x external SMA GPS antenna), dual power inputs.
FortiGate Rugged 60F	FGR-60F	Ruggedized, indoor, IP20, 4x GE RJ45 ports, 2x shared media ports (supports, 2x GE RJ45 ports or 2x SFP slots), 1x GE RJ45 bypass port pair (between PORT4 and WAN1), 1x RJ45 serial port (console), 1x DB9 serial port (data), 1x USB port, dual power inputs.
FortiGate Rugged 60F-3G4G	FGR-60F-3G4G	Ruggedized, indoor, IP20, 4x GE RJ45 ports, 2x shared media ports (supports, 2x GE RJ45 ports or 2x SFP slots), 1x GE RJ45 bypass port pair (between PORT4 and WAN1), 1x RJ45 serial port (console), 1x DB9 serial port (data), 1x USB port, 1 embedded 3G/4G LTE wireless WAN module (includes 2 SIM slots - Active/ Passive, 2x external SMA WWAN antennas), Passive GPS (includes 1x external SMA GPS antenna), dual power inputs.
FortiGate Rugged 70F	FGR-70F	Ruggedized, indoor, IP40, 4x GE RJ45 LAN ports, 1x GE RJ45 bypass port pair (between PORT3 and PORT4), 2x GE RJ45 WAN ports, 2x SFP slots, 1x RJ45 serial port (data), 1x RJ45 serial port (console), 1x USB port, 1x MicroSD card slot, dual power inputs.
FortiGate Rugged 70F-3G4G	FGR-70F-3G4G	Ruggedized, indoor, IP40, 4x GE RJ45 LAN ports, 1x GE RJ45 bypass port pair (between PORT3 and PORT4), 2x GE RJ45 WAN ports, 2x SFP slots, 1x RJ45 serial port (data), 1x RJ45 serial port (console), 1x USB port, 1x MicroSD card slot, 1x embedded 3G/4G LTE wireless WAN module (includes, 2x SIM slots - Active/Passive, 2x external SMA WWAN antennas), Passive GPS (includes 1x external SMA GPS antenna), dual power inputs.
FortiGate Rugged 70G-5G-DUAL	FGR-70G-5G-DUAL	Ruggedized, indoor, IP40, 4x GE RJ45 LAN ports, 1x GE RJ45 bypass port pair (between PORT1 and PORT2), 2x GE RJ45 WAN ports, 2x SFP slots, 1x RJ45 serial port (data), 1x RJ45 serial port (console), 1x USB port, 1x MicroSD card slot, 2x embedded 5G cellular wireless WAN module (includes, 2x SIM slots - Active/Active, 8x external SMA WWAN antennas), Passive GPS (includes 1x external SMA GPS antenna), dual power inputs.
Optional Accessories		
1 GE SFP RJ45 Transceiver Module, -40°C to 85°C operation	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module, SMF, -40°C to 85°C operation	FN-TRAN-LX	1 GE SFP LX transceiver module, -40°C to 85°C, over SMF, for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module, MMF, -40°C to 85°C operation	FR-TRAN-SX	1 GE SFP SX transceiver module, -40°C to 85°C, over MMF, for all systems with SFP and SFP/SFP+ slots.
1 GE SFP Transceiver Module, 90 km range, -40°C to 85°C operation	FR-TRAN-ZX	1 GE SFP transceivers, -40°C to W85°C operation, 90 km range for all systems with SFP slots.
100base-FX SFP Transceiver Module	FS-TRAN-FX	100 Mb multimode SFP transceiver module, -40°C to 85°C, 2 km range for systems with SFP Slots and capable of 10/100 Mb mode selection.
FortiPSU Rugged DIN Rail 240W PSU	SP-RGDIN-240-PS	Pack of 2 units - DIN Rail Rugged PSU 90-264VAC/106V-300VDC Input, 240W/54V Nominal Output, -30°C to 70°C.

OT Ordering Guide

Fortinet's OT ordering guide offers high-level mapping of solutions aligned with the Purdue Model based deployment architecture, allowing end-users and partners to select suitable solutions for their OT cybersecurity requirements. It contains a non-exhaustive list of the best-selling Fortinet products suited for OT cybersecurity use-cases and requirements.

Click here to access the ordering guide.

OT Security Solutions Hub

Visit the OT Security Solutions Hub for additional technical information on Fortinet solutions for operational technology.

FortiGuard Protection 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		

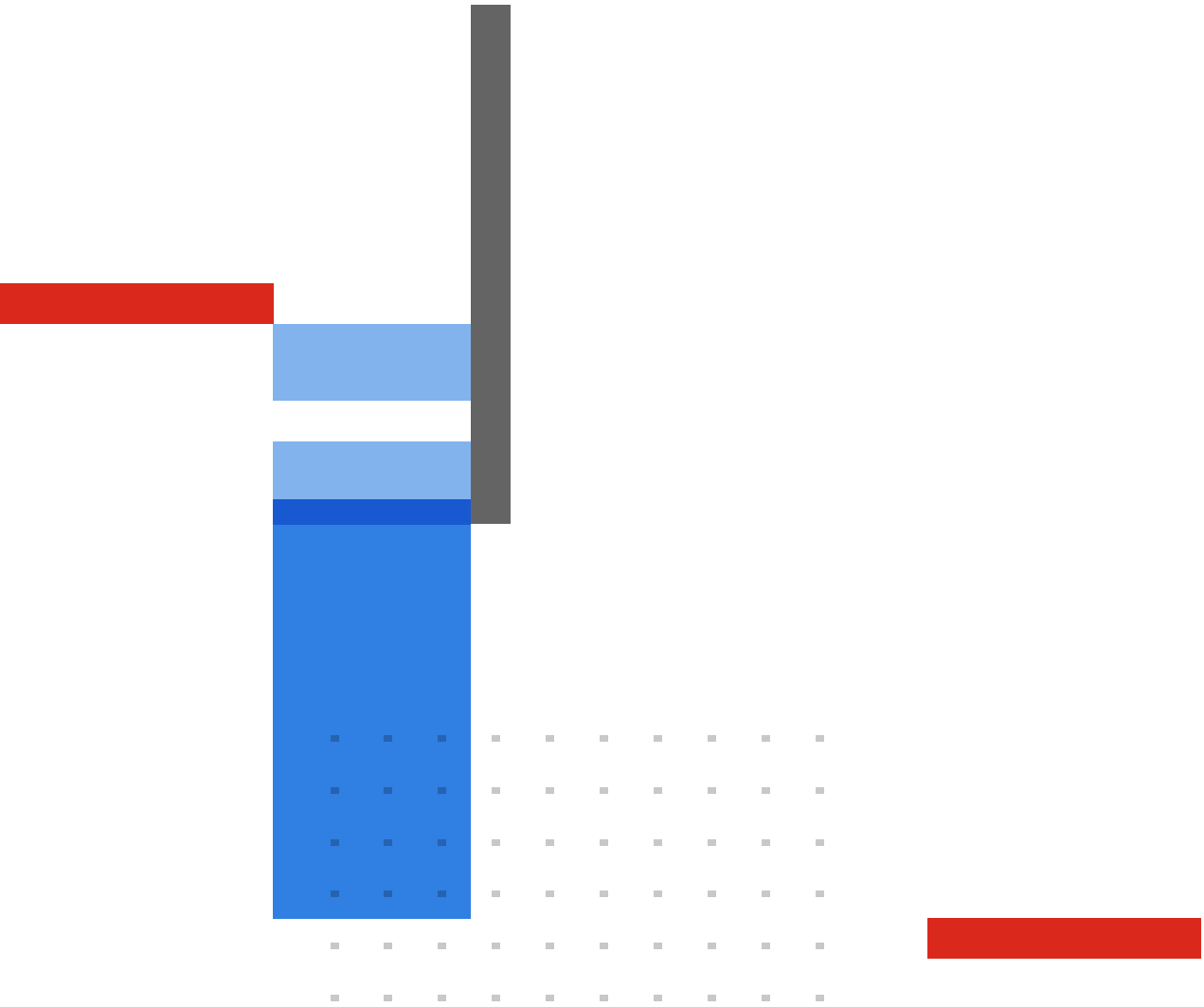
1. Full features available when running FortiOS v7.4.1
2. Desktop models only.
3. Features not supported on FGR-50G and FGR-60F series starting with FortiOS v7.4.4. It is recommended to use FortiOS v7.2.x LTS release to access these features on the affected models.

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.

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

January 30, 2025

FGR-DAT-R47-20250130