

# FortiGate Rugged Firewalls

FGR-60F, FGR-60F-3G4G, FGR-70F, and FGR-70F-3G4G



## Highlights

**Ruggedized Appliance** with fanless design ensures reliable operations in harsh conditions

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

**Enterprise Security** with consolidated AI-powered FortiGuard 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

## 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 next-gen firewalls 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.

Model	IPS	NGFW	Threat Protection	Interfaces
FGR-60F FGR-60F-3G4G	950 Mbps	550 Mbps	500 Mbps	Multiple GE RJ45, 2 SFP slots, 1 bypass pair   Variant with 3G4G Modem and GPS
FGR-70F FGR-70F-3G4G	975 Mbps	950 Mbps	580 Mbps	Multiple GE RJ45, 2 SFP slots, 1 bypass pair   Variant with 3G4G Modem and GPS   Digital I/O Module



Available in



Rugged Appliance

## FortiOS Everywhere

### FortiOS, Fortinet's Advanced Operating System

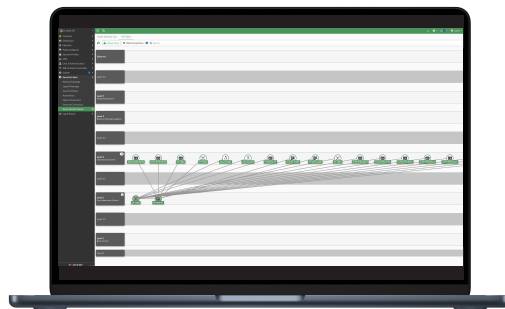
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

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.

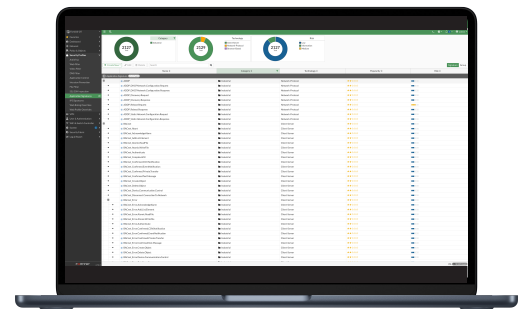
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more. It provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

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

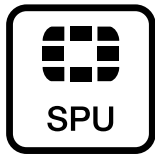


*OT focused dashboard for assets and analytics*



*Visibility and control for OT applications and protocols*

## 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

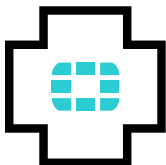


### Secure SD-WAN ASIC SOC4

- 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

### 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.



### 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



### 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 50+ 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

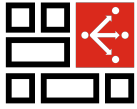
- Network segmentation implements the concept of security zones and conduits and prevent unauthorized access to critical OT assets, the firewall acts as a conduit between different zones and offers secure pathway for communication
  - Network segmentation limits the impact of any security incidents that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



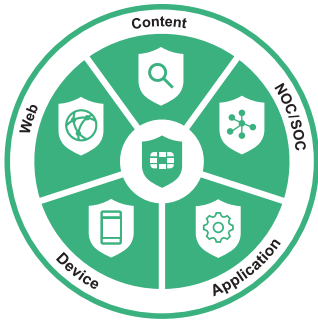
### Secure SD-WAN

- FortiGate 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



## 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 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 OT 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, 24x7 SOC analyst experts, managed firewall and endpoint functions, and alert triage.

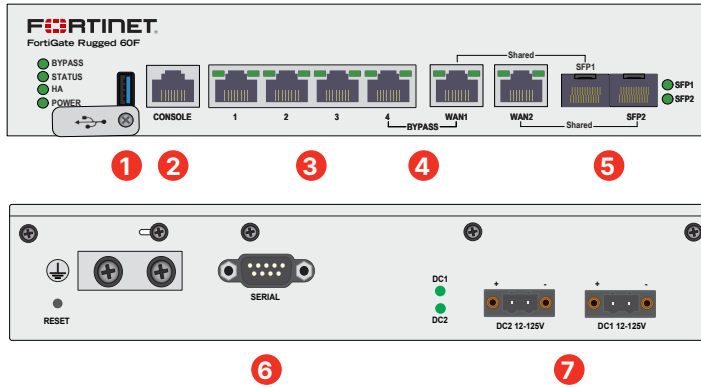
### Fabric Rating Security Best Practices

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

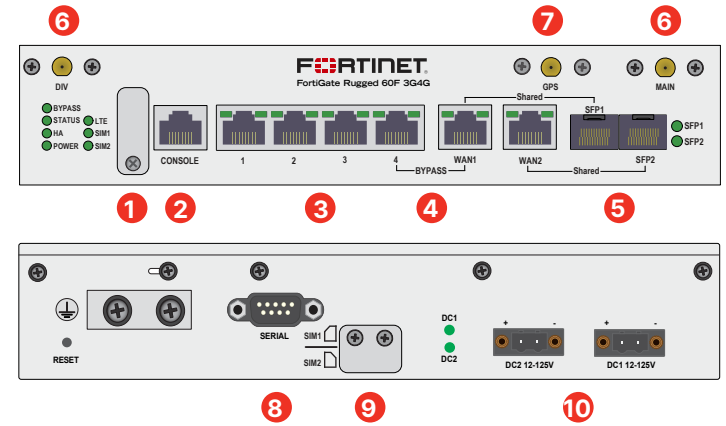


## Hardware

### FortiGate Rugged 60F



### FortiGate Rugged 60F-3G4G



### Interfaces

- 1x USB Port
- 1x RJ45 Console Port
- 4x GE RJ45 Ports
- 1x GE RJ45 Bypass Port Pair (PORT4 and WAN1)\*
- 2x GE RJ45/SFP Shared Media Ports
- 1x DB9 Serial Port (RS-232)
- 2x DC Power Inputs (Redundant Failover)

\* NOTE: WAN1/WAN2 and SFP1/SFP2 are shared interfaces

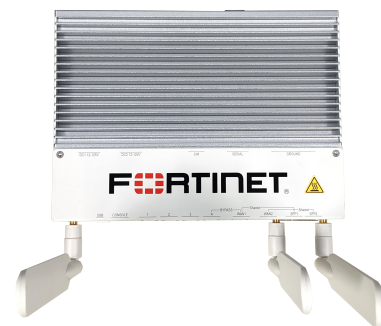
### Interfaces

- 1x USB Port
- 1x RJ45 Console Port
- 4x GE RJ45 Ports
- 1x GE RJ45 Bypass Port Pair (PORT4 and WAN1)\*
- 2x GE RJ45/SFP Shared Media Ports
- 2x SMA Antennae Connections for Cellular Wireless
- 1x SMA Antenna Connection for GPS
- 1x DB9 Serial Port (RS-232)
- 1x Integrated 3G/4G LTE Modem (Dual SIM - Active/Passive)
- 2x DC Power Inputs (Redundant Failover)

\* NOTE: WAN1/WAN2 and SFP1/SFP2 are shared interfaces



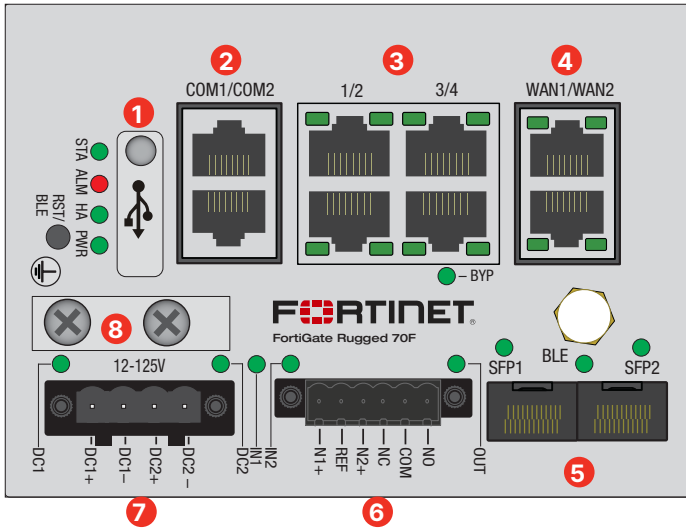
FortiGate Rugged 60F



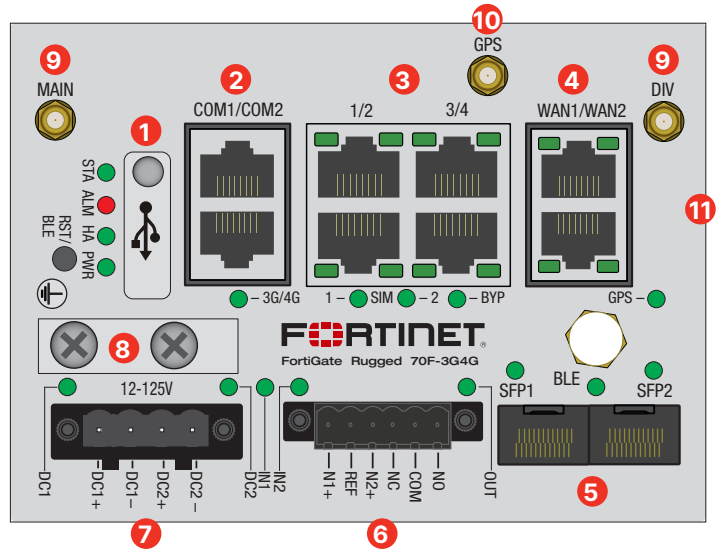
FortiGate Rugged 60F-3G4G

# Hardware

## FortiGate Rugged 70F



## FortiGate Rugged 70F-3G4G

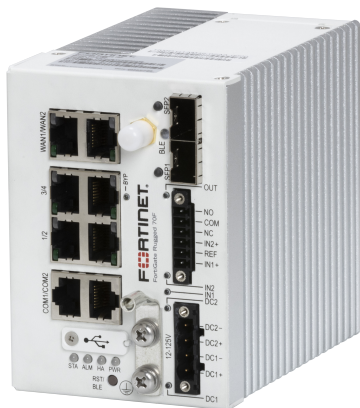


### Interfaces: FGR-70F, FGR-70F-3G4G

- 1x USB Port
- 2x RJ45 Serial Ports, COM1: Console, COM2: Data
- 4x GE RJ45 LAN Ports (PORT3 and PORT4 supports bypass)
- 2x GE RJ45 WAN Ports
- 2x GE SFP Slots
- 1x Digital I/O Module for Alarms
- 2x DC Power Inputs (Redundant)
- 1x Grounding Point

### Interfaces: FGR-70F-3G4G

9. 2x SMA Antennae Connections for Cellular Wireless
10. 1x SMA Antenna Connection for GPS
11. 1x Integrated 3G/4G LTE Modem (Dual SIM - Active/Passive)



FortiGate Rugged 70F



FortiGate Rugged 70F-3G4G





## Specifications

	FGR-60F	FGR-60F-3G4G	FGR-70F	FGR-70F-3G4G
<b>Interfaces and Modules</b>				
GE RJ45 Interfaces	4	4	6	6
Bypass GE RJ45 Port Pair	PORT4 and WAN1	PORT4 and WAN1	PORT3 and PORT4	PORT3 and PORT4
Dedicated GE SFP Slots	No	No	2	2
GE RJ45/SFP Shared Media Pairs	2	2	No	No
Serial Interface	1 DB9	1 DB9	1 RJ45	1 RJ45
USB (Client / Server)	1	1	1	1
RJ45 Console Port	1	1	1	1
Cellular Modem	No	3G / 4G LTE, GPS	No	3G / 4G LTE, GPS
Bluetooth Low Energy (BLE)	No	No	Yes	Yes
Transceivers Included	No	No	No	No
Processor	FortiSoC4	FortiSoC4	FortiSoC4	FortiSoC4
Trusted Platform Module (TPM)	Yes	Yes	Yes	Yes
Digital I/O Module (DIO)	No	No	Yes	Yes
<b>System Performance and Capacity</b>				
IPv4 Firewall Throughput (1518* / 512 / 64 byte UDP packets)	6/6/5.95 Gbps	6/6/5.95 Gbps	8/8/8 Gbps	8/8/8 Gbps
Firewall Latency (64 byte, UDP)	3.10 µs	3.10 µs	6.71 µs	6.71 µs
Firewall Throughput (Packets Per Second)	8.9 Mpps	8.9 Mpps	12 Mpps	12 Mpps
Concurrent Sessions (TCP)	600 000	600 000	1 M	1 M
New Sessions/Second (TCP)	19 000	19 000	35 000	35 000
Firewall Policies	5000	5000	5000	5000
IPsec VPN Throughput (512 byte) <sup>1</sup>	3.5 Gbps	3.5 Gbps	6.5 Gbps	6.5 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200	200	200	200
Client-to-Gateway IPsec VPN Tunnels	500	500	500	500
SSL-VPN Throughput	400 Mbps	400 Mbps	450 Mbps	450 Mbps
Concurrent SSL-VPN Users (Recommended Maximum)	100	100	100	100
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	460 Mbps	460 Mbps	500 Mbps	500 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	300	300	380	380
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	70 000	70 000	90 000	90 000
Application Control Throughput (HTTP 64K)	1.3 Gbps	1.3 Gbps	1.1 Gbps	1.1 Gbps
Virtual Domains (Default / Maximum)	10 / 10	10 / 10	10 / 10	10 / 10
Maximum Number of FortiAPs (Total / Tunnel)	30 / 10	30 / 10	64 / 32	64 / 32
Maximum Number of FortiTokens	500	500	500	500
Maximum Number of FortiSwitches	16	16	16	16
High Availability Configurations	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering

\*Measured using 1518 byte UDP packets

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

<sup>1</sup> IPsec VPN performance test uses AES256-SHA256.

<sup>2</sup> IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

<sup>3</sup> SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

<sup>4</sup> NGFW performance is measured with Firewall, IPS and Application Control enabled.

<sup>5</sup> Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

<sup>6</sup> AC adapter not supported.

<sup>7</sup> AC adapter not supported. Requires fabricated DC cables (refer to QuickStart Guide).

<sup>8</sup> DC cables are not included.



## Specifications

	FGR-60F	FGR-60F-3G4G	FGR-70F	FGR-70F-3G4G
<b>System Performance — Enterprise Traffic Mix</b>				
IPS Throughput <sup>2</sup>	950 Mbps	950 Mbps	975 Mbps	975 Mbps
NGFW Throughput <sup>2,4</sup>	550 Mbps	550 Mbps	950 Mbps	950 Mbps
Threat Protection Throughput <sup>2,5</sup>	500 Mbps	500 Mbps	580 Mbps	580 Mbps
<b>Dimensions and Power</b>				
Height x Width x Length (inches)	1.68 x 8.50 x 6.70	1.68 x 8.50 x 6.70	4.8 x 3.2 x 4.4	4.8 x 3.2 x 4.4
Height x Width x Length (mm)	42.7 x 216 x 170	42.7 x 216 x 170	122 x 80.5 x 111	122 x 80.5 x 111
Weight	3.85 lbs (1.75 kg)	4.06 lbs (1.84 kg)	2.87 lbs (1.3 kg)	2.87 lbs (1.3 kg)
Form Factor	Desktop/ DIN-rail/ Wall Mount	Desktop/ DIN-rail/ Wall Mount	DIN-rail	DIN-rail
Antennae (Height x Width)		205 mm x 25 mm		205 mm x 25 mm
IP Rating	IP20	IP20	IP40	IP40
Power Supply <sup>6,7,8</sup>	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.	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	16 W / 18 W	18.3 W / 19.9 W
Maximum Current	12V DC / 2A	12V DC / 2A	12V DC / 1.5A	12V DC / 1.67A
Heat Dissipation	72 BTU/h	82 BTU/h	62 BTU/h	68 BTU/h
<b>Operating Environment</b>				
Operating Temperature	-40°–167°F (-40°–75°C)	-40°–167°F (-40°–75°C)	-40°–167°F (-40°–75°C)	-40°–167°F (-40°–75°C)
Storage Temperature	-40°–167°F (-40°–75°C)	-40°–167°F (-40°–75°C)	-40°–167°F (-40°–75°C)	-40°–167°F (-40°–75°C)
Humidity	5%–95% non-condensing	5%–95% non-condensing	5%–95% non-condensing	5%–95% non-condensing
Operating Altitude	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 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.

<sup>1</sup> IPsec VPN performance test uses AES256-SHA256.

<sup>2</sup> IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

<sup>3</sup> SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

<sup>4</sup> NGFW performance is measured with Firewall, IPS and Application Control enabled.

<sup>5</sup> Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

<sup>6</sup> AC adapter not supported.

<sup>7</sup> AC adapter not supported. Requires fabricated DC cables (refer to QuickStart Guide).

<sup>8</sup> DC cables are not included.



# Specifications

	FGR-60F	FGR-60F-3G4G	FGR-70F	FGR-70F-3G4G
<b>Industry Compliance and Certifications</b>				
<b>Electric Power Industry</b>	IEC 61850-3 and IEEE 1613 Certified	IEC 61850-3 and IEEE 1613 Certified	IEC 61850-3 and IEEE 1613 Certified	IEC 61850-3 and IEEE 1613 Certified
<b>EMC</b>	EN 55032:2015, Class A EN 55035: 2017 EN IEC 61000-6-4:2019 IEC 61850-3:2013	EN 55032:2015, Class A EN 55035: 2017 EN IEC 61000-6-4:2019 IEC 61850-3:2013 EN 301 489-1 V2.2.3 Draft EN 301 489-52 V1.1.0 (2016-11)	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) ETSI EN 301 908-1 V15.1.1 (2021-09) EN 55032:2015, Class A IEC 61850-3:2013	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) ETSI EN 301 908-1 V15.1.1 (2021-09) EN 55032:2015, Class A IEC 61850-3:2013
<b>Health and Safety</b>	IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 IEC 62368-1:2018, 3rd Ed. EN IEC 62368-1:2020	IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 IEC 62368-1:2018, 3rd Ed. EN IEC 62368-1:2020	IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 IEC 62368-1:2018, 3rd Ed. EN IEC 62368-1:2020	IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 IEC 62368-1:2018, 3rd Ed. EN IEC 62368-1:2020
<b>Maritime Industry<sup>1</sup></b>	IEC 60945:2002 4th Ed. DNV GL Type Approved	IEC 60945:2002 4th Ed. DNV GL Type Approved		
<b>Regulatory Compliance</b>	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	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/cUL, CB
<b>RF</b>		Draft ETSI EN 301 489-19 V2.2.0 (2020-09) ETSI EN 301 489-52 V1.2.1 (2021-11) EN 301 908-1 V13.1.1 (2019-11) EN 301 908-2 V13.1.1 EN 301 908-13 V13.1.1 EN 303 413 V1.2.1 (2021-04)	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	ETSI EN 300 328 V2.2.2 (2019-07) EN 301 908-1 V13.1.1 (2019-11) EN 301 908-2 V13.1.1 EN 301 908-13 V13.1.1 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
<b>RoHS</b>	EN IEC 6300:2018 EN 50581:2012	EN IEC 6300:2018 EN 50581:2012	EN IEC 6300:2018 EN 50581:2012	EN IEC 6300:2018 EN 50581:2012
<b>Rolling Stock Industry</b>	EMC, Shock and Vibration Compliant EN 50121-1:2017 EMC EN 50121-4:2016 EMC IEC60068-2-27:2008 Shock IEC 60068-2-6:2007 Vibration	EMC Compliant EN 50121-1:2017 EMC EN 50121-4:2016 EMC	EN 50155:2017 EMC, Shock, and Vibration Certified	EN 50155:2017 EMC, Shock, and Vibration Certified

1. Maritime certification is only available for Gen3 release of FGR-60F and FGR-60F-3G4G.

	FGR-60F-3G4G	FGR-70F-3G4G
<b>Cellular Wireless Regional Compatibility</b>		
<b>Maximum Tx Power</b>	20 dBm	20 dBm
<b>Regions</b>	All Regions	All Regions
<b>Modem Model</b>	Sierra Wireless EM7565 (2 SIM Slots, Active/Passive)	Sierra Wireless EM7565 (2 SIM Slots, Active/Passive)
<b>LTE</b>	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, B9, B12, B13, B18, B19, B20, B26, B28, B29, B30, B32, B41, B42, B43, B46, B48, B66
<b>UMTS/HSPA+</b>	B1, B2, B3, B4, B5, B6, B8, B9, B29	B1, B2, B3, B4, B5, B6, B8, B9, B29
<b>WCDMA</b>	No	No
<b>CDMA 1xRTT/EV-DO Rev A</b>	No	No
<b>GSM/GPRS/EDGE</b>	No	No
<b>Module Certifications</b>	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB
<b>Diversity</b>	Yes	Yes
<b>MIMO</b>	Yes	Yes
<b>GNSS Bias</b>	Yes	Yes



## Supported Industrial Protocols

### FortiGuard Industrial Security Service

- Allen-Bradley DF1
- Allen-Bradley PCCC
- BACnet
- CC-Link
- CN/IP CEA-852
- CoAP
- Common Industrial Protocol (CIP)
- DICOM
- Digi ADDP
- Digi RealPort (Net C/X)
- Direct Message Profile
- DNP3
- ECHONET Lite
- ECOM100
- ELCOM 90
- Emerson DeltaV
- Ether-S-Bus
- Ether-S-I/O
- EtherCAT
- Ethernet POWERLINK
- EtherNet/IP
- FactorySuite NMXSVC
- FL-net
- GE EGD
- GE SRTP (GE Fanuc)
- HART-IP
- HL7
- IEC 60870-5-104 (IEC 104)☞
- IEC 60870-6/TASE.2 (ICCP)
- IEC 61850 MMS
- IEC 62056 DLMS/COSEM
- IEC TR 61850-90-5 R-GOOSE
- IEC TR 61850-90-5 R-SV
- IEEE 1278.2 DIS
- IEEE C37.118 Synchrophasor
- ISO 9506 MMS
- KNXnet/IP (EIBnet/IP)
- LonTalk IEC14908-1 CNP
- Mitsubishi MELSEC
- Modbus TCP☞
- Moxa Modbus RTU☞
- Moxa UDP Device Discovery
- MQTT
- MTConnect
- Niagara Fox
- oBIX
- OCPP
- Omron FINS
- OPC AE
- OPC DA
- OPC HDA
- OPC UA
- OpenADR
- OSIsoft PI
- Profinet CBA
- Profinet IO
- RealPort DNP3☞
- Remote Operations Controller (ROC)
- Rockwell FactoryTalk
- RTPS
- SafetyNET p
- Schneider UMAS
- Siemens LOGO
- Siemens S7
- Siemens S7 1200
- Siemens S7 Plus
- Siemens SIMATIC CAMP
- STANAG 4406 Military Messaging
- STANAG 5066
- Triconex TriStation
- Veeder-Root ATG Access
- Vnet/IP

☞ Additional parameters supported for the signatures in the GUI (requires FortiOS v6.4 or above).

Visit <https://www.fortiguard.com/services/is> to view the latest list of industrial applications and protocols included in the FortiGuard Industrial Security Service.



## Ordering Information

Product	SKU	Description
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, embedded 3G/4G LTE wireless WAN module (includes, 2 SIM slots - Active/Passive, 2x external SMA WWAN antennae), 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, embedded 3G/4G LTE wireless WAN module (includes, 2x SIM slots - Active/Passive, 2x external SMA WWAN antennae), Passive GPS (includes, 1x external SMA GPS antenna), dual power inputs.
<b>Optional Accessories</b>		
1 GE SFP LX transceivers, SMF, -40°-85°C operation	FN-TRAN-LX	1 GE SFP LX transceiver module, -40°C-85°C, over SMF, for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX transceivers, MMF, -40°-85°C operation	FR-TRAN-SX	1 GE SFP SX transceiver module, -40°C-85°C, over MMF, for all systems with SFP and SFP/SFP+ slots.
1 GE SFP transceivers, 90 km range, -40-85°C operation	FR-TRAN-ZX	1 GE SFP transceivers, -40°C-85°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° to 85°C, 2 km range for systems with SFP Slots and capable of 10/100 Mb mode selection

## 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.



## FortiGuard Protection 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 <sup>1</sup>	•				
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 <sup>1</sup>					
	Internet Service (SaaS) DB Updates					
	GeoIP DB Updates					included with FortiCare Subscription
	Device/OS Detection Signatures					
	Trusted Certificate DB Updates					
	DDNS (v4/v6) Service					

<sup>1</sup> Available when running FortiOS 7.2



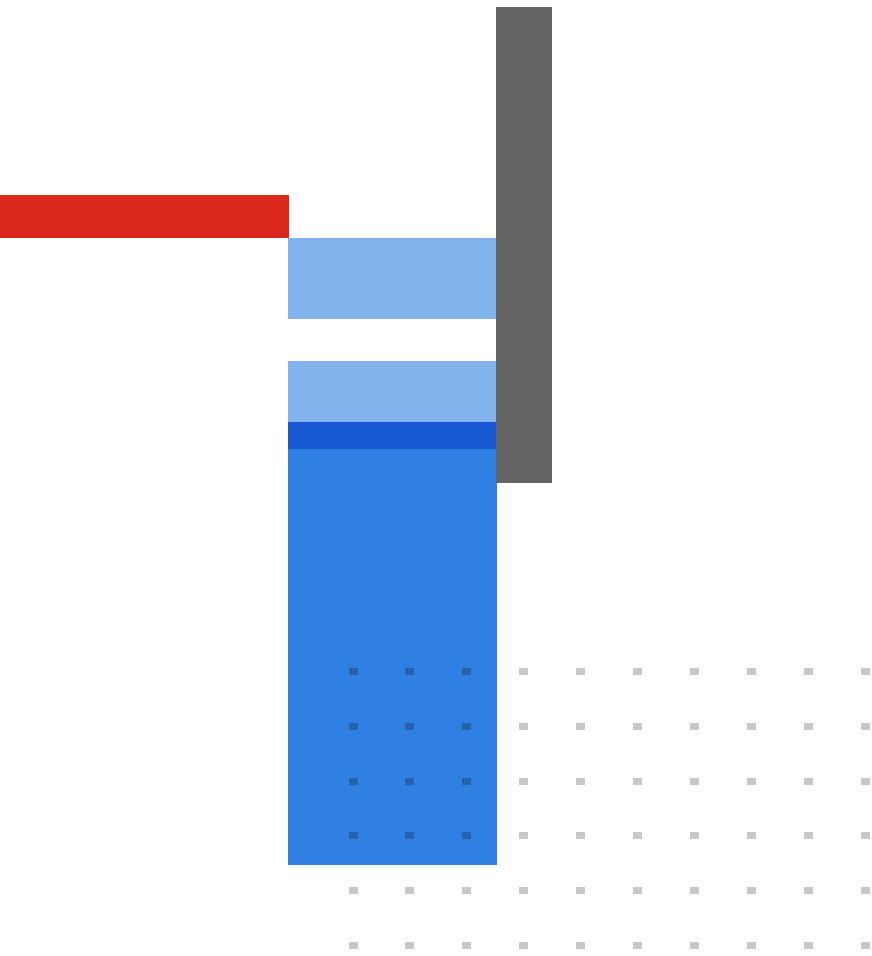
### FortiGuard Bundles

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.



### 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](http://www.fortinet.com)

Copyright © 2023 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 General Counsel, 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.

February 9, 2023

FGR-DAT-R28-20230209