

DATA SHEET

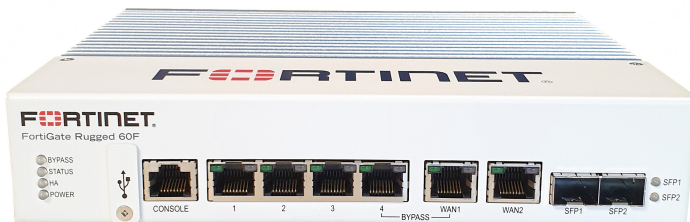
# FortiGate® Rugged Series

Available in:



Appliance

## Mission Critical Security Solutions for Industrial Environments



While traditional security solutions are designed and intended for the world of offices and corporations, the FortiGate Rugged Series offers an industrially-hardened, all-in-one security appliance that delivers specialized threat protection for securing critical industrial and control networks against malicious attacks.



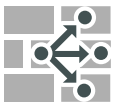
### Ruggedized Design

Fanless and use of robust components ensure reliable operation in harsh industrial environments.



### Consolidated Security Architecture

FortiGate running FortiOS consolidated security offers better protection and lower cost of ownership than multiple point products. Coupled with FortiGuard Industrial Security Service, it ensures that critical networks receive real-time protection.



### SD-WAN Capable

Supports reliable connectivity with lower costs via built in SD-WAN technologies.



### Ease of Management

Robust management systems that allow rapid provision and deployment, monitoring of device and threat status while providing actionable reports.

## PRODUCT OFFERINGS

### FGR-30D

Ruggedized compact security appliance with DIN mounting kit

### FGR-35D

Security appliance with IP67 rating for outdoor environment

### FGR-60F

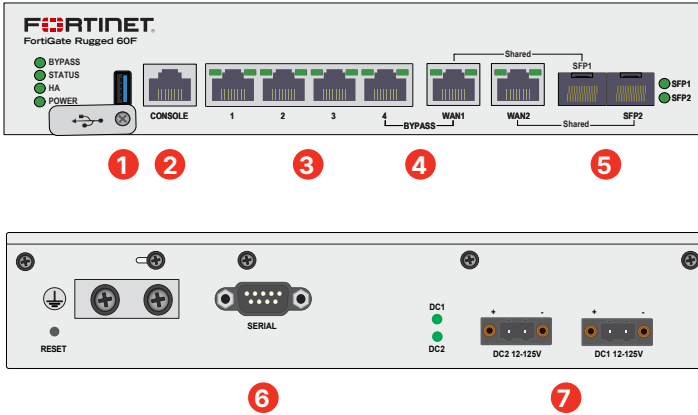
New SPU SoC4-powered for rugged and harsh environments

### FGR-60F-3G4G

Integrated 3G4G modem for industrial and mission-critical applications

# HARDWARE

## FortiGate Rugged 60F

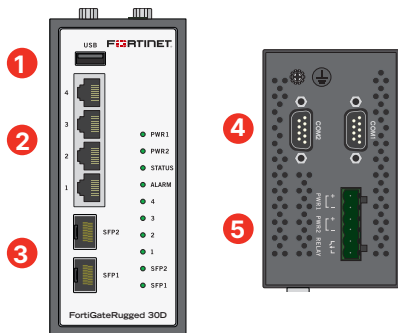


### Interfaces

1. 1x USB Port
2. 1x RJ45 Console Port
3. 4x GE RJ45 Ports
4. 1x GE RJ45 Bypass Port Pair (PORT4 & WAN1, default setting)\*
5. 2x GE RJ45/SFP Shared Media Ports
6. 1x DB9 Serial Port (RS-232)
7. 2x DC Power Inputs (Redundant Failover)

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

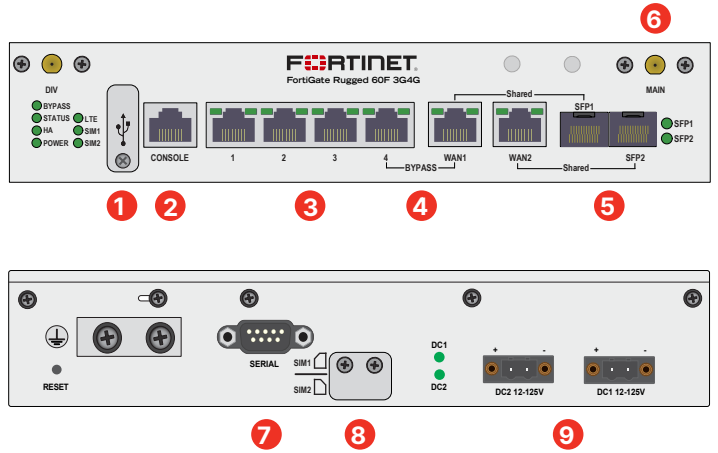
## FortiGate Rugged 30D



### Interfaces

1. 1x USB Port
2. 4x GE RJ45 Ports
3. 2x GE SFP Slots
4. 2x DB9 Serial Ports (Data/Console)
5. 2x Power Inputs, 1x Relay Connection

## FortiGate Rugged 60F-3G4G

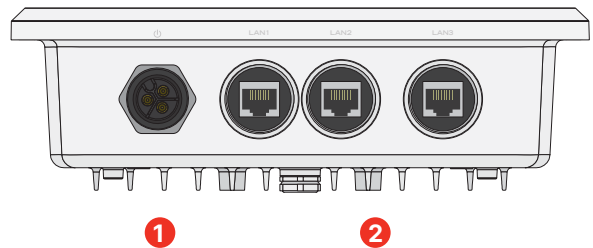


### Interfaces

1. 1x USB Port
2. 1x RJ45 Console Port
3. 4x GE RJ45 Ports
4. 1x GE RJ45 Bypass Port Pair (PORT4 & WAN1, default setting)\*
5. 2x GE RJ45/SFP Shared Media Ports
6. 2x SMA Antennae Connections
7. 1x DB9 Serial Port (RS-232)
8. 1x Integrated 3G/4G LTE Modem (Dual SIM - Active/Passive)
9. 2x DC Power Inputs (Redundant Failover)

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

## FortiGate Rugged 35D



### Interfaces

1. 1x Power Input
2. 3x GE RJ45 Ports



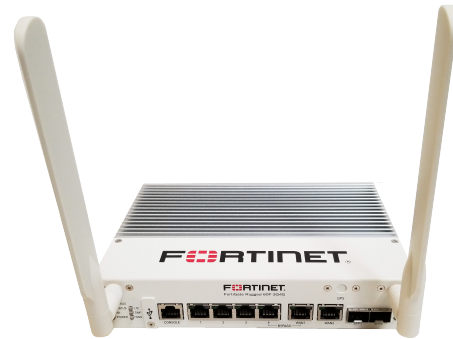
## HARDWARE

### Trusted Platform Module (FGR-60F Series)

The FortiGate Rugged 60F Series features an integrated hardware security module, also known as Trusted Platform Module (TPM), that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.



**FortiGate Rugged 60F**



**FortiGate Rugged 60F-3G4G**



**FortiGate Rugged 30D**



**FortiGate Rugged 35D**



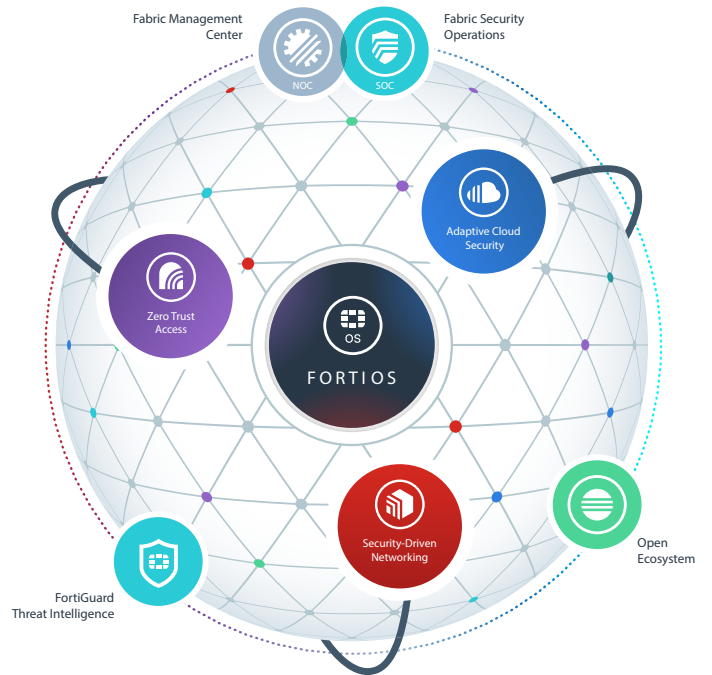
# FORTINET SECURITY FABRIC

## Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad:** Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated:** Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated:** Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



## FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoints, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7\* dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models consisting on appliances, software and As-a-Service with SASE, ZTNA, and other emerging cybersecurity solutions.

\* FortiOS 7 is not supported on FGR-30D and FGR-35D.

## SERVICES

### FortiGuard™ Security Services

FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.

### FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1,000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.



# SPECIFICATIONS

	FGR-30D	FGR-35D	FGR-60F	FGR-60F-3G4G
<b>Interfaces and Modules</b>				
GE RJ45 Interfaces	4	3	4	4
Bypass GE RJ45 Port Pair*	No	No	1*	1*
GE SFP Slots	2	No	No	No
GE RJ45/SFP Shared Media Pairs	No	No	2	2
DB9 Serial Interface	2	No	1	1
USB (Client / Server)	1	No	1	1
RJ45 Console Port	No	No	1	1
Cellular Modem	No	No	No	3G / 4G LTE
Transceivers Included	No	No	No	No
Processor	CPU	CPU	FortiSoC4	FortiSoC4
Trusted Platform Module (TPM)	No	No	Yes	Yes
<b>System Performance and Capacity</b>				
IPv4 Firewall Throughput (1518** / 512 / 64 byte UDP packets)	900 Mbps**	550 Mbps**	6/6/5.95 Gbps	6/6/5.95 Gbps
Firewall Latency (64 byte, UDP)	70.00 µs	90.00 µs	3.10 µs	3.10 µs
Firewall Throughput (Packets Per Second)	87 Kpps	52.5 Kpps	8.9 Mpps	8.9 Mpps
Concurrent Sessions (TCP)	750 000	750 000	600 000	600 000
New Sessions/Second (TCP)	5000	5000	19 000	19 000
Firewall Policies	5000	5000	5000	5000
IPsec VPN Throughput (512 byte) <sup>1</sup>	45 Mbps	45 Mbps	3.5 Gbps	3.5 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200	200	200	200
Client-to-Gateway IPsec VPN Tunnels	250	250	500	500
SSL-VPN Throughput	25 Mbps	25 Mbps	400 Mbps	400 Mbps
Concurrent SSL-VPN Users (Recommended Maximum)	80	80	100	100
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	50 Mbps	55 Mbps	460 Mbps	460 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	75	75	300	300
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	45 000	45 000	70 000	70 000
Application Control Throughput (HTTP 64K)	210 Mbps	230 Mbps	1.3 Gbps	1.3 Gbps
Virtual Domains (Default / Maximum)	5 / 5	5 / 5	10 / 10	10 / 10
Maximum Number of FortiAPs (Total / Tunnel)	2 / 2	2 / 2	30 / 10	30 / 10
Maximum Number of FortiTokens	20	20	500	500
Maximum Number of FortiSwitches	8	8	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

\*Default bypass port pair configuration is PORT4 and WAN1

\*\*Measured using 1518 byte UDP packets

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

- IPsec VPN performance test uses AES256-SHA256.
- IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
- SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

- NGFW performance is measured with Firewall, IPS and Application Control enabled.
- Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.
- AC adapter not supported.
- AC adapter not supported. Requires fabricated DC cables (refer to QuickStart Guide).
- DC cables are not included.



## SPECIFICATIONS

	FGR-30D	FGR-35D	FGR-60F	FGR-60F-3G4G
<b>System Performance — Enterprise Traffic Mix</b>				
IPS Throughput <sup>2</sup>	180 Mbps	210 Mbps	950 Mbps	950 Mbps
NGFW Throughput <sup>2,4</sup>	45 Mbps	65 Mbps	550 Mbps	550 Mbps
Threat Protection Throughput <sup>2,5</sup>	16 Mbps	16 Mbps	500 Mbps	500 Mbps
<b>Dimensions and Power</b>				
Height x Width x Length (inches)	5.49 × 4.13 × 2.36	3.07 × 10.04 × 10.04	1.68 × 8.50 × 6.70	1.68 × 8.50 × 6.70
Height x Width x Length (mm)	139.5 × 105 × 60	78 × 255.09 × 255.09	42.7 × 216 × 170	42.7 × 216 × 170
Weight	1.46 lbs (0.668 kg)	3.986 lbs (1.808 kg)	3.85 lbs (1.75 kg)	4.06 lbs (1.84 kg)
Form Factor	Desktop/ DIN-rail/ Wall Mount	Outdoor Wall/ Pole Mount	Desktop/ DIN-rail/ Wall Mount	Desktop/ DIN-rail/ Wall Mount
Antennae (Height x Width)				205 mm x 25 mm
IP Rating	IP20	IP67	IP20	IP20
Power Supply <sup>6,7,8</sup>	Dual inputs, total 6 pin terminal block (12–48V DC) DC cables are not included.	Terminal block (12–48V DC) 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)	15.55 W / 15.92 W	10.2 W / 10.5 W	15 W / 21 W	16 W / 24 W
Maximum Current	1.19A	0.83A	12V DC / 2A	12V DC / 2A
Heat Dissipation	54.29 BTU/h	35.81 BTU/h	72 BTU/h	82 BTU/h
<b>Operating Environment</b>				
Operating Temperature	-40–158°F (-40–70°C)	-40–140°F (-40–60°C)	-40–167°F (-40–75°C)	-40–167°F (-40–75°C)
Storage Temperature	-58–185°F (-50–85°C)	-58–185°F (-50–85°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 7400 ft (2250 m)	Up to 7400 ft (2250 m)
<b>Industry Compliance and Certifications</b>				
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	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/cUL, CB
Electric Power Industry	IEC 61850-3 and IEEE 1613 Emission Compliant	IEC 61850-3 and IEEE 1613 Emission Compliant	IEC 61850-3 and IEEE 1613 Certified	IEC 61850-3 and IEEE 1613 Certified
Rolling Stock Industry	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	EN 55032:2015, Class B EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013 EN 61850-3:2014	EN 55032:2015, Class A EN 55024:2010 EN 61000-3-2:2014 EN 61000-3-3:2013 EN 61850-3:2013 IEC/TS 61000-6-5:2001	EN 55032:2015, Class A EN 55024:2010 EN 55035: 2017 EN 61000-3-2:2014 EN 61000-3-3:2013 EN IEC 61000-6-4:2019 IEC 61850-3:2013	EN 55032:2015, Class A EN 55024:2010 EN 55035: 2017 EN 61000-3-2:2014 EN 61000-3-3:2013 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)
RF				EN 301 908-1 V13.1.1 (2019-11) EN 301 908-2 V13.1.1 EN 301 908-13 V13.1.1
Health and Safety	IEC 60950-1:2005, 2nd Ed. EN 60950-1:2006	IEC 60950-1:2005, 2nd Ed. EN 60950-1:2006 IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 IEC 60950-22:2005 EN 60950-22:2006 IEC 60529 Ed. 2.1 (2001-02) IP67	IEC 60950-1:2005, 2nd Ed. EN 60950-1:2006 IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014	IEC 60950-1:2005, 2nd Ed. EN 60950-1:2006 IEC 62368-1:2014, 2nd Ed. EN 62368-1:2014 EN 62311:2008 EN 50665:2017 EN 50385:2017 EN 62479:2010 EN 50663:2017
RoHS	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

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. AC adapter not supported.
7. AC adapter not supported. Requires fabricated DC cables (refer to QuickStart Guide).
8. DC cables are not included.



## SPECIFICATIONS

FGR-60F-3G4G	
<b>Regional Compatibility</b>	
<b>Maximum Tx Power</b>	20 dBm
<b>Regions</b>	All Regions
<b>Modem Model</b>	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
<b>UMTS/HSPA+</b>	B1, B2, B3, B4, B5, B6, B8, B9, B29
<b>WCDMA</b>	No
<b>CDMA 1xRTT/EV-DO Rev A</b>	No
<b>GSM/GPRS/EDGE</b>	No
<b>Module Certifications</b>	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB
<b>Diversity</b>	Yes
<b>MIMO</b>	Yes
<b>GNSS Bias</b>	Yes

## SUPPORTED INDUSTRIAL PROTOCOLS

### IPS and Application Control for Operational Technology / Industrial Control Systems

- ADDP
- Allen-Bradley PCCC
- BACnet
- CC-Link
- CIP
- CN/IP (EIA/CEA-852)
- CoAP
- DICOM
- DNP3 RealPort
- RealPort DNP3\*
- ECHONET Lite
- ELCOM 90
- Emerson DeltaV
- Ether-S-Bus
- EtherCAT Automation Protocol (EAP)
- Ethernet Global Data (GE EGD)
- Ethernet Powerlink
- EtherNet/IP
- FL-net
- GE SRTP (GE Fanuc)
- HART-IP
- HL7
- IEC 60870-5-104 (IEC-104)\*
- IEC 60870-6 (TASE.2/ICCP)
- IEC 61850 MMS
- IEC 61850 R-GOOSE
- IEC 61850 R-SV
- IEEE 1278.2 Distributed Interactive Simulation
- IEEE C37.118 Synchrophasor
- KNXnet/IP (EIBnet/IP)
- LonTalk/EIA-709.1
- Mitsubishi MELSEC
- Modbus TCP\*
- Modbus Unity
- MOXA
- MOXA Modbus RTU\*
- MQTT
- MTConnect
- Net C/X (Digi RealPort)
- Niagara Fox
- OPC Classic (DA, HDA, AE)
- OPC UA
- IEC 62056 (DLMS/COSEM)
- OpenADR
- OSIsoft PI System
- PROFINET
- RTPS
- SafetyNet p
- Siemens S7, S7Plus, LOGO
- STANAG 4406
- STANAG 5066
- TriStation
- Vedder-Root

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



## ORDERING INFORMATION

Product	SKU	Description
FortiGate Rugged 30D	FGR-30D	Ruggedized, indoor, IP20, 4x GE RJ45 ports, 2x GE SFP slots, 2x DB9 serial ports, 1x USB port, dual power inputs.
FortiGate Rugged 35D	FGR-35D	Ruggedized, outdoor, IP67, 3x GE RJ45 ports, single power input.
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), dual power inputs.
Optional Accessories		
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, 90km 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.

## BUNDLES



### FortiGuard Bundle

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.

Bundles	Enterprise Protection	SMB Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	24x7	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video <sup>1</sup> Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•			
FortiGuard IoT Detection Service	•			
FortiGuard Industrial Security Service	•			
FortiConverter Service	•			
FortiGate Cloud Subscription		•		

1. Available when running FortiOS 7.0



www.fortinet.com

Copyright © 2022 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.