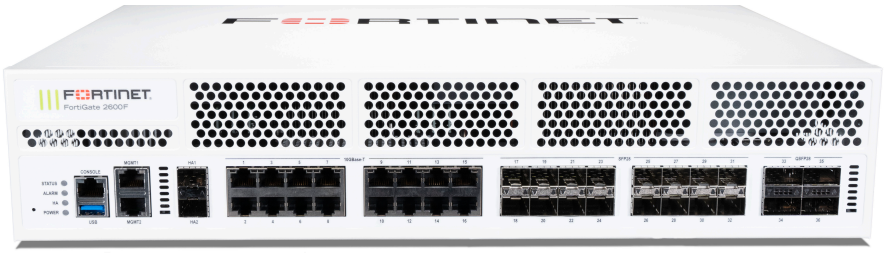
DATA SHEET

FortiGate® 2600F Series

FG-2600F/-DC and FG-2601F/-DC

Next Generation Firewall
Segmentation
Secure Web Gateway
IPS
Mobile Security



The FortiGate 2600F series delivers high-performance threat protection and SSL inspection for large enterprises and service providers, with the flexibility to be deployed at the enterprise/cloud edge, in the data center core or internal segments. The multiple high-speed interfaces, high port density, superior security efficacy and high throughput of the 2600F series keep your network connected and secure.

Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

Performance

- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification

- Independently tested and validated best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

Security Fabric

- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

Firewall	IPS	NGFW	Threat Protection	Interfaces
198 Gbps	**24 Gbps**	**19 Gbps**	**17 Gbps**	Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP and 100GE QSFP28 / 40 GE QSFP+ slots

Refer to specification table for details

DEPLOYMENT

Next Generation Firewall (NGFW)

- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with Industry-validated IPS security effectiveness, low latency and optimized network performance
- Automatically block threats on decrypted traffic using the Industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns

Secure Web Gateway(SWG)

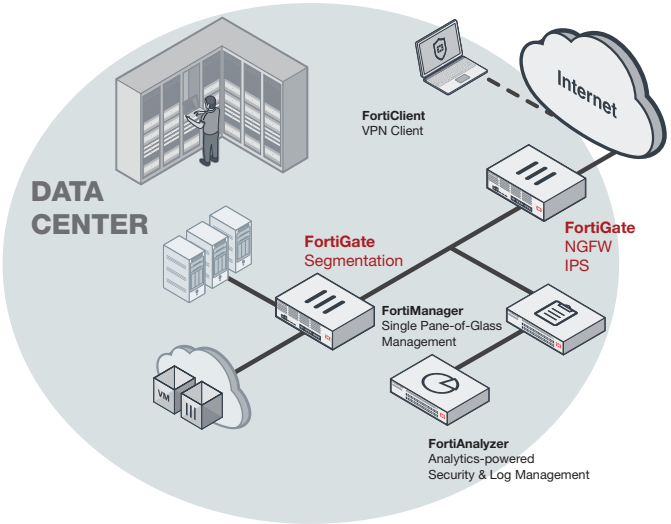
- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL's and domains
- Prevent data loss and discover user activity to known and unknown cloud applications
- Block DNS requests against malicious domains
- Multi-layered advanced protection against zero-day malware threats delivered over the web

IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric

Mobile Security for 4G, 5G, and IOT

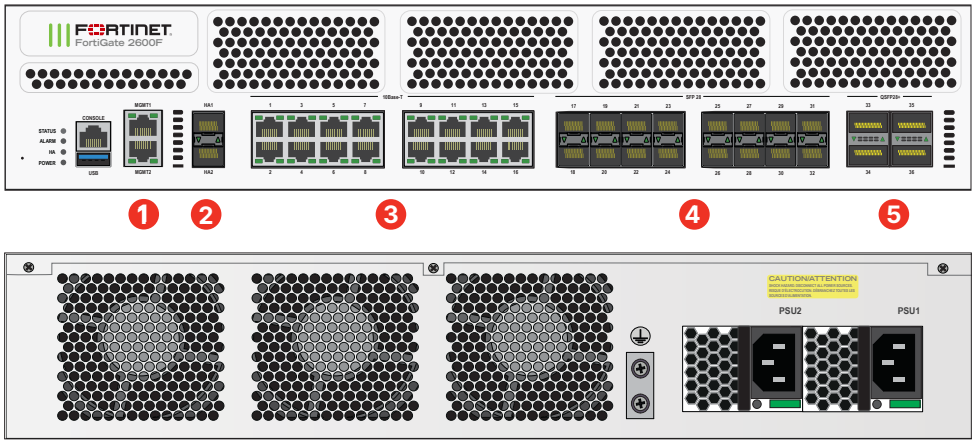
- SPU accelerated, high performance CGNAT and IPv6 migration option including: NAT44, NAT444, NAT64/DNS64, NAT46 for 4G Gi/sGi and 5G N6 connectivity and security
- RAN Access Security with highly scalable and best performing IPsec aggregation and control security gateway (SecGW)
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- 4G and 5G security for user and data plane traffic including SCTP, GTP-U, and SIP that provides protection against attacks
- High-speed interfaces to enable deployment flexibility



Data Center Deployment
(IPS/NGFW, Intent-based Segmentation)

HARDWARE

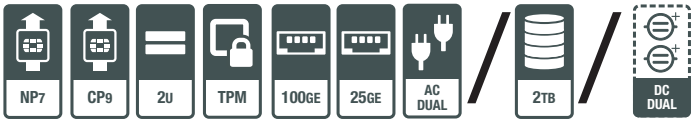
FortiGate 2600F Series



Interfaces

1. 2x GE RJ45 MGMT Ports
2. 2× 10 GE SFP+ / GE SFP HA Slots
3. 16× 10 GE / GE RJ45 Ports
4. 16× 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots
5. 4× 100 GE QSFP28 / 40 GE QSFP+ Slots

Hardware Features



Hyperscale Firewall License

Empower organizations by unlocking further performance boosts with this perpetual license. The Hyperscale Firewall License will enable the hardware acceleration of CGNAT features by utilizing the latest SPU NP7. These features include hardware session setup, firewall session logging, and NAT.

Powered by SPU

- Fortinet's custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck

Network Processor

Fortinet's new, breakthrough SPU NP7 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

Fortinet's ninth generation custom SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection.

Trusted Platform Module (TPM)

The FortiGate 2600F 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.

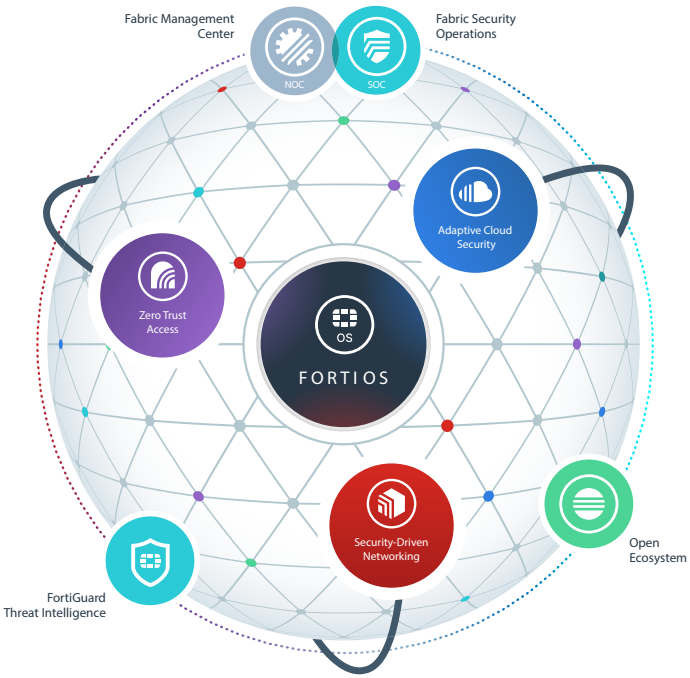
FORTINET SECURITY FABRIC

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 and 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 endpoint, 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 of Hardware, Software, and Software As-a-Service with SASE and ZTNA, among others.

SERVICES

FortiGuard™ Security Services

FortiGuard Labs offer 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 1000 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

	FG 2600F/-DC	FG 2601F/-DC
Interfaces and Modules		
Hardware Accelerated 10 GE / GE RJ45 Ports	16	
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots	16	
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots	4	
Hardware Accelerated 10 GE SFP+ / GE SFP HA Slots	2	
GE RJ45 Management Ports	2	
USB 3.0 Port	1	
Console RJ45 Port	1	
Onboard Storage	–	2× 1 TB NVME SSD
Trusted Platform Module (TPM)	Yes	
Included Transceivers	2x SFP+ (SR 10 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	24 Gbps	
NGFW Throughput [2, 4]	19 Gbps	
Threat Protection Throughput [2, 5]	17 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	198 / 196 / 120 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	198 / 196 / 120 Gbps	
Firewall Latency (64 byte, UDP)	3.41 µs	
Firewall Throughput (Packet per Second)	180 Mpps	
Concurrent Sessions (TCP)	24 Million / 40 Million*	
New Sessions/Second (TCP)	1 Million / 2 Million*	
Firewall Policies	100 000	
IPsec VPN Throughput (512 byte) [1]	55 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	20 000	
Client-to-Gateway IPsec VPN Tunnels	100 000	
SSL-VPN Throughput	16 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30 000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	20 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	16 000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	2.7 Million	
Application Control Throughput (HTTP 64K) [2]	64 Gbps	
CAPWAP Throughput (HTTP 64K)	62.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 500	
Maximum Number of FortiSwitches Supported	196	
Maximum Number of FortiAPs (Total / Tunnel)	4096 / 2048	
Maximum Number of FortiTokens	20 000	
Maximum Number of Registered FortiClients	20 000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG 2600F/-DC	FG 2601F/-DC
Dimensions and Power		
Height x Width x Length (inches)	3.5 × 17.25 × 21.1	
Height x Width x Length (mm)	88.4 × 438 × 536	
Weight	30.6 lbs (13.9 kg)	30.9 lbs (14.0 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2 RU	
AC Power Supply	100–240VAC, 47/63 Hz	
AC Current (Maximum)	6A	
DC Power Supply	-48V to -60V DC	
DC Current (Maximum)	15A	
Power Consumption (Average / Maximum)	416 W / 510 W	420.3 W / 513.7 W
Heat Dissipation	1740 BTU/h	1754 BTU/h
Redundant Power Supplies	Yes, Hot Swappable	
Operating Environment and Certifications		
Operating Temperature	32°–104°F (0°–40°C)	
Storage Temperature	-31°–158°F (-35°–70°C)	
Humidity	10%–90% non-condensing	
Noise Level	71.72 dBA	
Forced Airflow	Side and Front to Back	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, USGv6/IPv6	

* Requires Hyperscale Firewall License

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.

ORDERING INFORMATION

Product	SKU	Description
FortiGate 2600F	FG-2600F	4 × 100GE/40GE QSFP28 slots, 16 × 25GE/10GE SFP28 slots, 16 × 10GE RJ45 ports, 2× 10G SFP+ HA slots, 2× 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies.
FortiGate 2601F	FG-2601F	4 × 100GE/40GE QSFP28 slots, 16 × 25GE/10GE SFP28 slots, 16 × 10GE RJ45 ports, 2× 10G SFP+ HA slots, 2× 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with 2TB onboard storage.
FortiGate 2600F-DC	FG-2600F-DC	4 × 100GE/40GE QSFP28 slots, 16 × 25GE/10GE SFP28 slots, 16 × 10GE RJ45 ports, 2× 10G SFP+ HA slots, 2× 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual DC power supplies.
FortiGate 2601F-DC	FG-2601F-DC	4 × 100GE/40GE QSFP28 slots, 16 × 25GE/10GE SFP28 slots, 16 × 10GE RJ45 ports, 2× 10G SFP+ HA slots, 2× 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual DC power supplies with 2TB onboard storage.
Hyperscale Firewall License FG1KF2KF	LIC-FGT-HYPSC-1K2K	Hyperscale Firewall License for FortiGate FG1800F/FG1801F/ FG2600F/ FG2601F Series for hardware acceleration.

Optional Accessories	SKU	Description
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.
25 GE SFP28 Transceiver Module, Short Range	FN-TRAN-SFP28-SR	25 GE SFP28 transceiver module, short range for all systems with SFP28 slots.
25 GE SFP28 Transceiver Module, Long Range	FN-TRAN-SFP28-LR	25 GE SFP28 transceiver module, long range for all systems with SFP28 slots.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceivers, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Short Range, BiDi	FN-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceivers, short range BiDi for systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceivers, long range for all systems with QSFP+ slots.
40 GE QSFP+ to 4× 10 GE SFP+ optical breakout, 1 meter	FG-TRAN-QSFP-4XSFP	40 GE QSFP+ parallel breakout MPO to 4x LC connectors, 1 m reach, transceivers not included.
100 GE QSFP28 Transceivers, Short Range	FN-TRAN-QSFP28-SR	100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots.
100 GE QSFP28 Transceivers, Long Range	FN-TRAN-QSFP28-LR	100 GE QSFP28 transceivers, 4 channel parallel fiber, long range for all systems with QSFP28 slots.
100 GE QSFP28 Transceivers, CWDM4	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 slots.
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1100/1101E, FG-1200D, FG-1500D/-DC, FG-1800F, FG-2000E, FG-2500E, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC and FG-3950B/-DC.
AC Power Supply	SP-FG1800F-PS	AC power supply for FG-1800/1801F and FG-2600/2601F.
DC Power Supply	SP-FG1800F-DC-PS	DC power supply for FG-1800/1801F and FG-2600/2601.
40GE QSFP+ Passive Direct Attach Cable 1m	SP-CABLE-FS-QSFP+1	40GE QSFP+ Passive Direct Attach Cable, 1m for Systems with QSFP+ slots.
40GE QSFP+ Passive Direct Attach Cable 3m	SP-CABLE-FS-QSFP+3	40GE QSFP+ Passive Direct Attach Cable, 3m for Systems with QSFP+ slots.
40GE QSFP+ Passive Direct Attach Cable 5m	SP-CABLE-FS-QSFP+5	40GE QSFP+ Passive Direct Attach Cable, 5m for Systems with QSFP+ 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	Unified Threat Protection	Advanced Threat Protection
FortiCare	24×7	24×7	24×7
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[1] Filtering Service	•	•	
FortiGuard Antispam Service	•	•	
FortiGuard Security Rating Service	•		
FortiGuard IoT Detection Service	•		
FortiGuard Industrial Service	•		
FortiConverter Service	•		

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.

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 censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA (https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf) and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy (https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf).

FG-2600F-DAT-R14-20220602