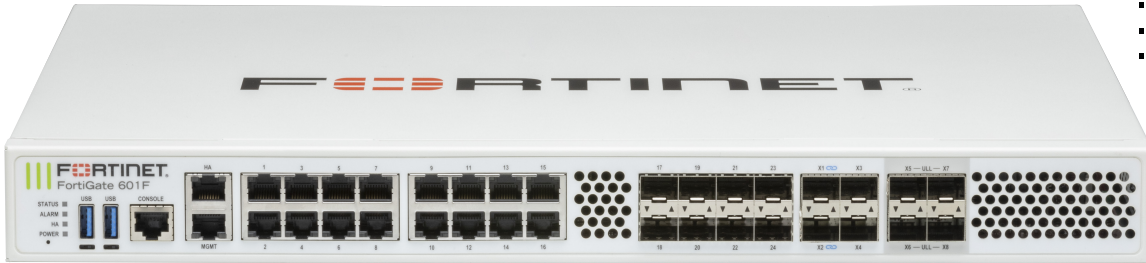


# FortiGate® 600F Series

FG-600F and FG-601F

**Next Generation Firewall  
Secure SD-WAN  
Secure Web Gateway**



The FortiGate 600F series provides an application-centric, scalable, and secure SD-WAN solution with Next Generation Firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or branch level. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet’s Security-Driven Networking approach provides tight integration of the network to the new generation of security.

**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 (VDMs) 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
139 Gbps	14 Gbps	11.5 Gbps	10.5 Gbps	Multiple 25GE SFP28, 10GE SFP+, GE SFP Slots and GE RJ45

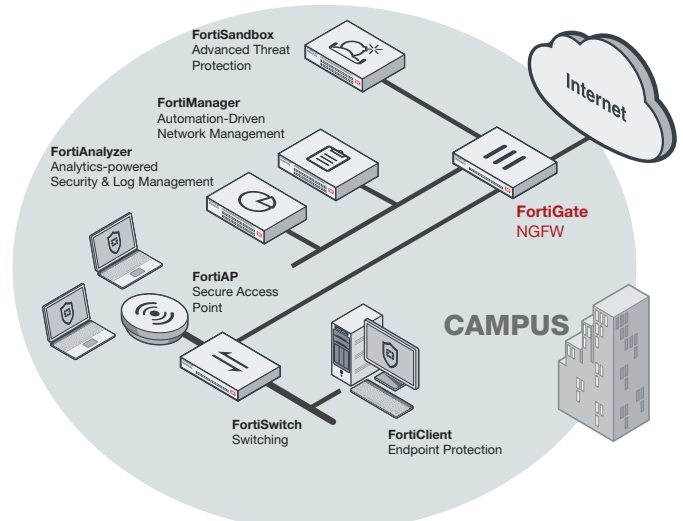
\* Refer to specification table for details

## 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, and applications across the entire attack surface, and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers 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

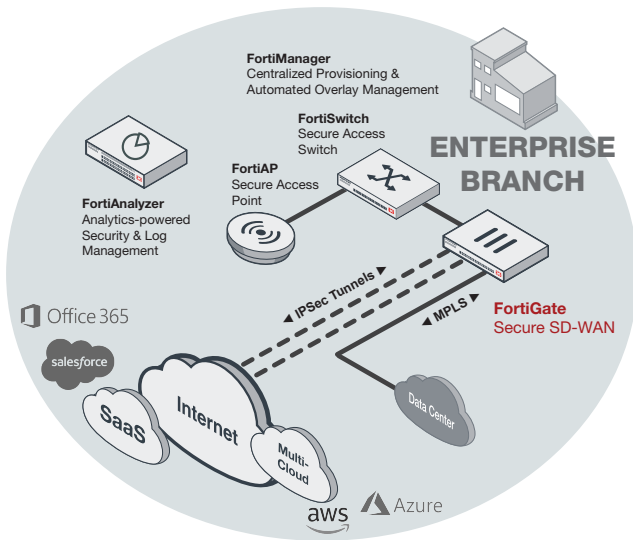


Campus Deployment (NGFW)



### Secure SD-WAN

- Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport
- Accelerated multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based and real-time bandwidth compute-based traffic steering
- Automated overlay tunnels provides encryption and abstracts physical hybrid WAN making it simple to manage.
- Simplified and intuitive workflow with FortiManger for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identifies anomalies
- Strong security posture with next generation firewall and real-time threat protection

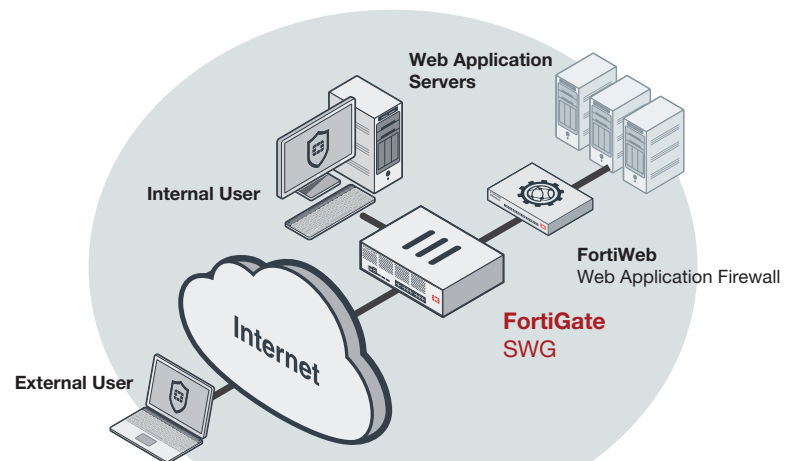


Enterprise Branch Deployment (Secure SD-WAN)



### 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 URLs 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

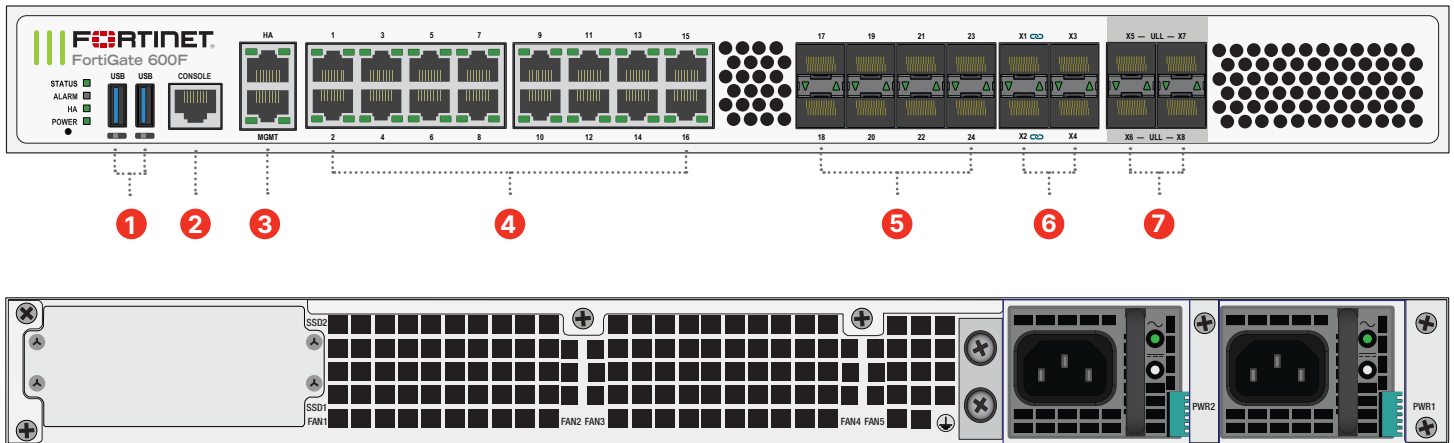


Secure Web Gateway Deployment (SWG)



# HARDWARE

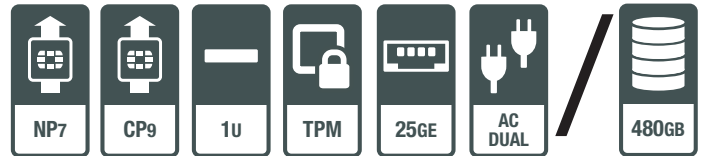
## FortiGate 600F/601F




### Interfaces

1. 2x USB Ports
2. 1x Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 16x GE RJ45 Ports
5. 8x GE SFP Slots
6. 4x 10GE/GE SFP+/SFP Slots
7. 4x 25GE/10GE SFP28/SFP+ Ultra Low Latency Slots

### Hardware Features



### Powered by SPU



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.



# 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 user
- **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 HW, Software and 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 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

	FG-600F	FG-601F
<b>Interfaces and Modules</b>		
Hardware Accelerated GE RJ45 Interfaces		16
Hardware Accelerated GE SFP Slots		8
Hardware Accelerated 10GE SFP+ Slots		4
Hardware Accelerated 25GE SFP28/10GE SFP+/ GE SFP Ultra Low Latency Slots		4
GE RJ45 MGMT/HA Ports		2
USB Ports		2
RJ45 Console Port		1
Onboard Storage	0	2x 240 GB SSD
Included Transceivers	2x SFP (SX 1 GE)	
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		14 Gbps
NGFW Throughput <sup>2,4</sup>		11.5 Gbps
Threat Protection Throughput <sup>2,5</sup>		10.5 Gbps
<b>System Performance and Capacity</b>		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	139 / 137.5 / 70 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	139 / 137.5 / 70 Gbps	
Firewall Latency (64 byte, UDP)	4.12 μs / 2.5 μs*	
Firewall Throughput (Packet per Second)	105 Mpps	
Concurrent Sessions (TCP)	8 Million	
New Sessions/Second (TCP)	550 000	
Firewall Policies	10 000	
IPsec VPN Throughput (512 byte) <sup>1</sup>	55 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	50 000	
SSL-VPN Throughput <sup>6</sup>	4.3 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10 000	
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	9 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	7500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	840 000	
Application Control Throughput (HTTP 64K) <sup>2</sup>	32 Gbps	
CAPWAP Throughput (HTTP 64K)	64.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	96	
Maximum Number of FortiAPs (Total / Tunnel)	1024 / 512	
Maximum Number of FortiTokens	5000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

\* Latency based on Ultra Low Latency (ULL ports)

	FG-600F	FG-601F
<b>Dimensions and Power</b>		
Height x Width x Length (inches)	1.75 × 17.0 × 15.0	
Height x Width x Length (mm)	44.45 × 432 × 380	
Weight	15.6 lbs (7.1 kg)	16.2 lbs (7.35 kg)
Form Factor	Rack Mount, 1 RU	
AC Power Consumption (Average / Maximum)	169 W / 255 W	174 W / 260 W
AC Power Input	100–240V AC, 50/60Hz	
AC Current (Maximum)	6A@100V	
Heat Dissipation	871 BTU/h	888 BTU/h
Redundant Power Supplies (Hot Swappable)	Yes (comes with 2PSU default)	
<b>Operating Environment and Certifications</b>		
Operating Temperature	32°–104°F (0°–40°C)	
Storage Temperature	-31°–158°F (-35°–70°C)	
Humidity	5%–90% non-condensing	
Noise Level	55 dBA	
Airflow	Side and Front to Back	
Operating Altitude	Up to 10 000 ft. (3048 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, USGv6/IPv6	

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

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

4. NGFW performance is measured with Firewall, IPS and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.
6. Uses RSA-2048 certificate.



## ORDERING INFORMATION

PRODUCT	SKU	DESCRIPTION
FortiGate 600F	FG-600F	4 × 25G SFP28 slots, 4 × 10GE SFP+ slots, 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, SPU NP7 and CP9 hardware accelerated, dual AC power supplies.
FortiGate 601F	FG-601F	4 × 25G SFP28 slots, 4 × 10GE SFP+ slots, 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, SPU NP7 and CP9 hardware accelerated, 480GB onboard SSD storage, dual AC power supplies.
<b>Optional Accessories</b>		
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.
25GE SFP28 Transceiver Module, Short Range	FN-TRAN-SFP28-SR	25GE/10GE Dual Rate SFP28 transceiver module, short range for all systems with SFP28/SFP+ slots
25GE SFP28 Transceiver Module, Long Range	FN-TRAN-SFP28-LR	25GE SFP28 transceiver module, long range for all systems with SFP28 slots
AC Power Supply	SP-FG400F-PS	AC power supply for FG-400/401F, FG-600/601F, power cable SP-FGPCOR-XX sold separately.

## 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 <sup>1</sup> 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 all 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 illegal 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](https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf)).