

DATA SHEET

FortiGate® 80F Series

FG-80F, 80F-Bypass, and FG-81F

**Secure SD-WAN
Next Generation Firewall**



The FortiGate 80F series provides an application-centric, scalable, and secure SD-WAN solution in a compact, fanless, desktop form factor for enterprise branch offices and mid-sized businesses. 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 for best-in-class 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 Fortinet’s 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
10 Gbps	1.4 Gbps	1 Gbps	900 Mbps	Multiple GE RJ45 Variants with internal storage and LAN Bypass

DEPLOYMENT



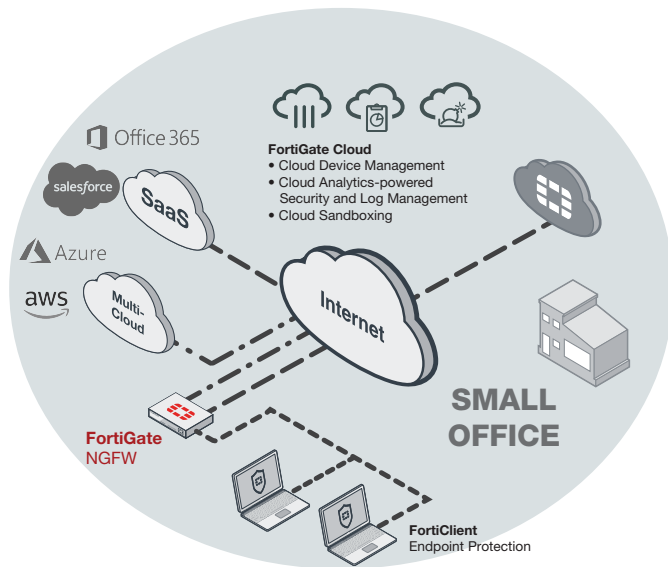
Next Generation Firewall (NGFW)

- 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

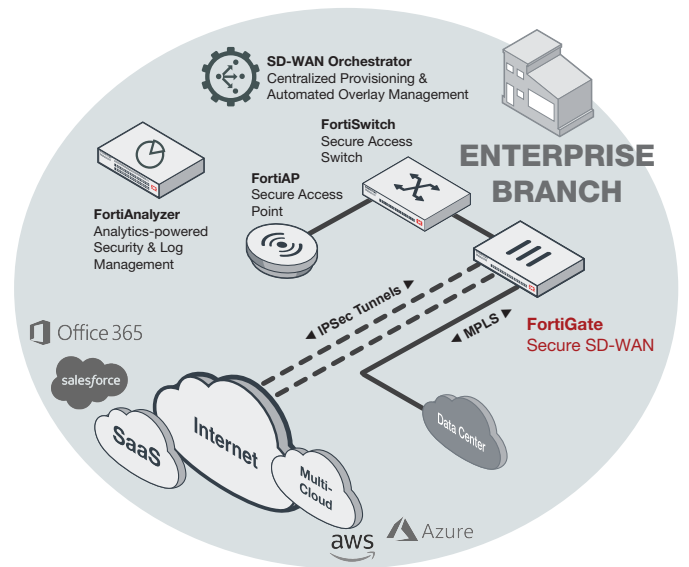


Secure SD-WAN

- 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 SD-WAN orchestrator 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



Small Office Deployment (NGFW)

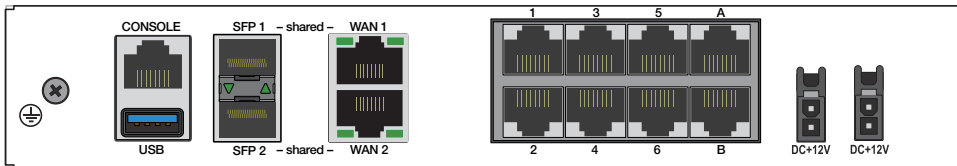
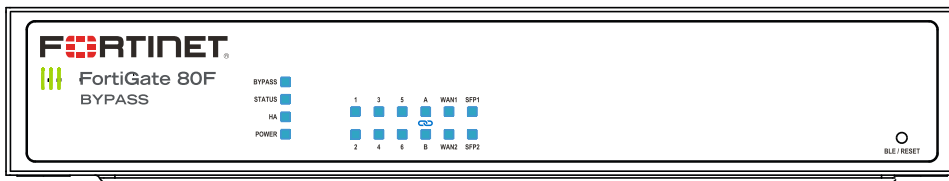


Enterprise Branch Deployment (Secure SD-WAN)



HARDWARE

FortiGate 80F/80F-Bypass/81F



Interfaces

1. 2x GE RJ45/SFP Shared Media Ports
2. 1x Bypass GE RJ45 Port Pair
(WAN1 and Port1, default configuration)*
3. 6x GE RJ45 Ports
4. 2x GE RJ45 FortiLink Ports

*80F-Bypass model only

Hardware Features



Powered by Purpose-built 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

The FortiGate-80F 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.

Bypass WAN/LAN Mode

The FortiGate-80F-Bypass offers a pair of bypass ports that help organizations avoid network communication interruption due to device faults and improve network reliability.

3G/4G WAN Connectivity

The FortiGate 80F Series includes a 3.0 USB port that allows you to plug in a compatible third-party 3G/4G USB modem, providing additional WAN connectivity or a redundant link for maximum reliability.

Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.



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 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 consisting on appliances, software and As-a-Service with SASE, ZTNA and other emerging cybersecurity solutions.

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

	FORTIGATE 80F	FORTIGATE 80F-BYPASS	FORTIGATE 81F
Hardware Specifications			
GE RJ45/SFP Shared Media Pairs	2	2	2
GE RJ45 Internal Ports	6	6	6
GE RJ45 FortiLink Ports (Default)	2	2	2
Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)	–	1	–
USB Ports 3.0	1	1	1
Console (RJ45)	1	1	1
Internal Storage	–	–	1× 128 GB SSD
System Performance — Enterprise Traffic Mix			
IPS Throughput 2		1.4 Gbps	
NGFW Throughput 2, 4		1 Gbps	
Threat Protection Throughput 2, 5		900 Mbps	
System Performance			
Firewall Throughput (1518 / 512 / 64 byte UDP packets)		10/10/7 Gbps	
Firewall Latency (64 byte UDP packets)		3.23 μs	
Firewall Throughput (Packets Per Second)		10.5 Mpps	
Concurrent Sessions (TCP)		1.5 Million	
New Sessions/Second (TCP)		45,000	
Firewall Policies		5,000	
IPsec VPN Throughput (512 byte) 1		6.5 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels		200	
Client-to-Gateway IPsec VPN Tunnels		2,500	
SSL-VPN Throughput		950 Mbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		200	
SSL Inspection Throughput (IPS, avg. HTTPS) 3		715 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) 3		700	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3		100,000	
Application Control Throughput (HTTP 64K) 2		1.8 Gbps	
CAPWAP Throughput (HTTP 64K)		9 Gbps	
Virtual Domains (Default / Maximum)		10 / 10	
Maximum Number of FortiSwitches Supported		16	
Maximum Number of FortiAPs (Total / Tunnel Mode)		96 / 48	
Maximum Number of FortiTokens		500	
High Availability Configurations		Active / Active, Active / Passive, Clustering	
Dimensions			
Height x Width x Length (inches)		1.5 × 8.5 × 6.3	
Height x Width x Length (mm)		38.5 × 216 × 160	
Weight		1.1 lbs (2.4 kg)	
Form Factor		Desktop/Wall Mount/Rack Tray	

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, URL filtering, and Malware Protection with sandboxing enabled.



SPECIFICATIONS

	FORTIGATE 80F	FORTIGATE 80F-BYPASS	FORTIGATE 81F
Operating Environment and Certifications			
Input Rating	12Vdc, 3A (dual redundancy optional)		
Power Required (Redundancy Optional)	Powered by up to 2 External DC Power Adapters (1 adapter included), 100–240V AC, 50/60 Hz		
Power Consumption (Average / Maximum)	12.6W / 15.4W	12.6W / 15.4W	13.5W / 16.5W
Heat Dissipation	52.55 BTU/h	52.55 BTU/h	56.30 BTU/h
Operating Temperature	32–104°F (0–40°C)		
Storage Temperature	-31–158°F (-35–70°C)		
Humidity	10–90% non-condensing		
Noise Level	Fanless 0 dBA		
Operating Altitude	Up to 7,400 ft (2,250 m)		
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB		
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN		

ORDERING INFORMATION

Product	SKU	Description
FortiGate 80F	FG-80F	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports
FortiGate 81F	FG-81F	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, 128GB onboard storage
FortiGate 80F-Bypass	FG-80F-Bypass	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, may be configured with 1 pair of LAN bypass
Accessories	SKU	Description
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, 80E/81E and 80F/81F
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-40F series, FG/FWF-60F series, FG-80F, FG-81F and FG-80F-Bypass
Transceivers	SKU	Description
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.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/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	360 Protection	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	ASE ¹	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 ² Filtering Service	•	•	•	•
FortiGuard Antispam Service	•	•	•	•
FortiGuard Security Rating Service	•	•	•	•
FortiGuard IoT Detection Service	•	•	•	•
FortiGuard Industrial Service	•	•	•	•
FortiConverter Service	•	•	•	•
SD-WAN Orchestrator Entitlement	•	•	•	•
SD-WAN Cloud Assisted Monitoring	•	•	•	•
SD-WAN Overlay Controller VPN Service	•	•	•	•
Fortinet SOCaaS	•	•	•	•
FortiAnalyzer Cloud	•	•	•	•
FortiManager Cloud	•	•	•	•

1. 24×7 plus Advanced Services Ticket Handling

2. Available when running FortiOS 7.0



www.fortinet.com

Copyright © 2021 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.