DATA SHEET

FortiGate 80F Series

FortiGate 80F, 80F-Bypass and 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
- Prevents and detects against known attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services
- Proactively blocks unknown sophisticated attacks in real-time with the Fortinet Security Fabric integrated AI-powered FortiSandbox

Performance

- Engineered for Innovation using Fortinet's purpose-built security processors (SPU) to deliver the industry's best threat protection performance and ultra-low latency
- Provides industry-leading performance and protection for SSL encrypted traffic including the first firewall vendor to provide TLS 1.3 deep inspection

Certification

- Independently tested and validated best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs, ICSA, Virus Bulletin, and AV Comparatives

Networking

- Dynamic Path Selection over any WAN transport to provide better application experience based on self-healing SD-WAN capabilities
- Advanced routing, Scalable VPN, multi-cast and IPV4/IPV6 forwarding powered by purpose-built network processors

Management

- SD-WAN Orchestration provides intuitive and simplified work-flow for centralized management and provisioning of business policies in a few easy clicks
- Expedited deployment with Zero touch provisioning well-suited for large and distributed infrastructure
- Automated VPN tunnels for flexible hub-to-spoke and full-mesh deployment at scale to provide bandwidth aggregation and encrypted WAN paths
- Predefined compliance checklists analyze the deployment and highlight best practices to improve the 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
- Automatically builds Network Topology visualizations which discover IoT devices and provide complete visibility into Fortinet and Fabric-ready partner products

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

Refer to the specifications table for details

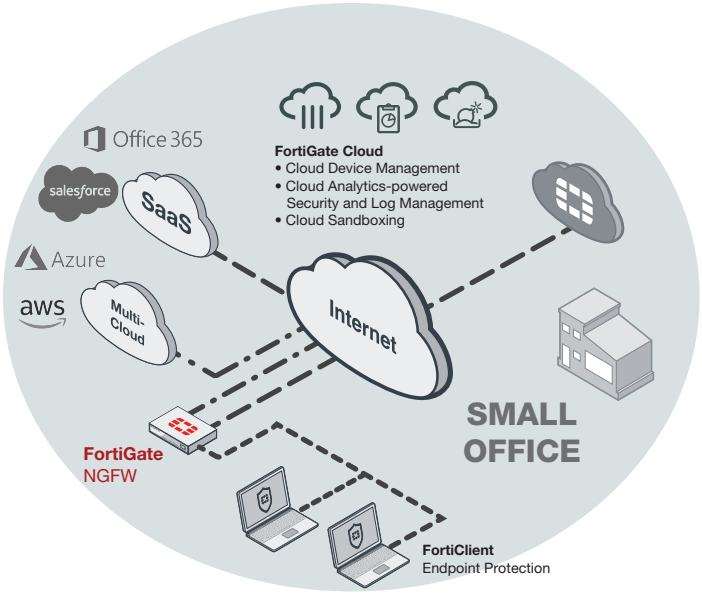
Deployment

Next Generation Firewall (NGFW)

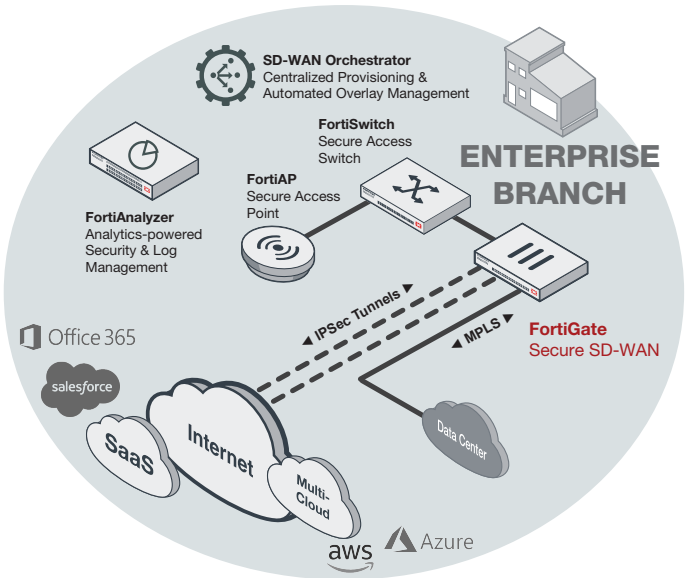
- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS 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 identify anomalies
- Strong security posture with next generation firewall and real-time threat protection



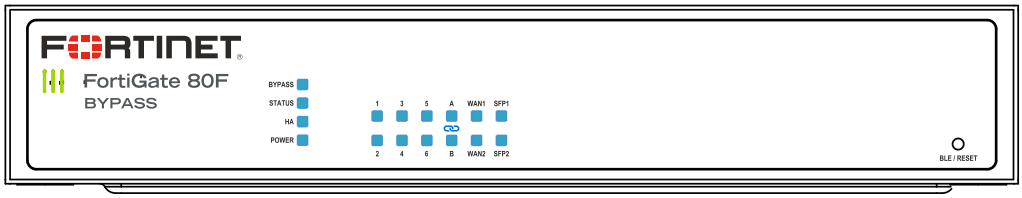
FortiGate 80F deployment in Small Office (NGFW)

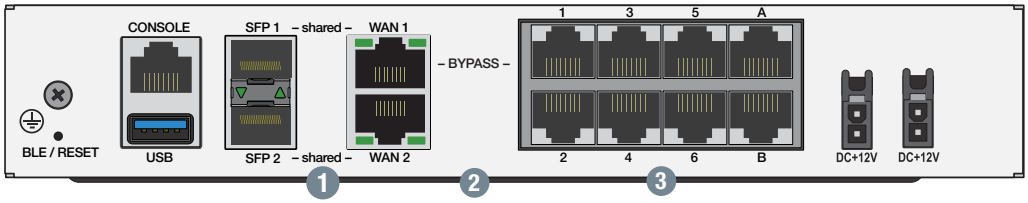


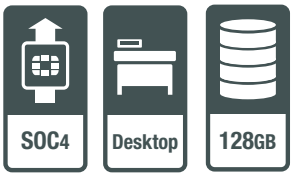
FortiGate 80F deployment in Enterprise Branch (Secure SD-WAN)

Hardware

FortiGate 80F/80F-Bypass/81F







Interfaces

1. 2x GE RJ45/SFP Shared Media Ports
2. 1x Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)*
3. 8x GE RJ45 Ports

*80F-Bypass model only

Powered by Purpose-built Secure SD-WAN ASIC SOC4

SPU

- 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

Bypass WAN/LAN Mode

The FortiGate-80F-Bypass offers a pair of bypass port pair that helps organizations to 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

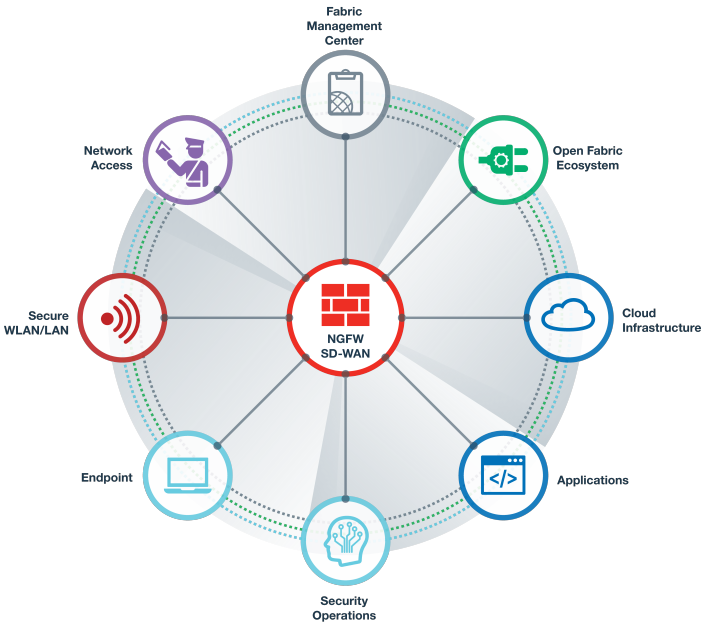
Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Fortinet Security Fabric

Security Fabric

The Security Fabric is the cybersecurity platform that enables digital innovations. It delivers broad visibility of the entire attack surface to better manage risk. Its unified and integrated solution reduces the complexity of supporting multiple-point products, while automated workflows increase operational speeds and reduce response times across the Fortinet deployment ecosystem. The Fortinet Security Fabric overs the following key areas under a single management center:

- **Security-Driven Networking** that secures, accelerates, and unifies the network and user experience
- **Zero Trust Network Access** that identifies and secures users and devices in real-time, on and off of the network
- **Dynamic Cloud Security** that protects and controls cloud infrastructures and applications
- **AI-Driven Security Operations** that automatically prevents, detects, isolates, and responds to cyber threats



FortiOS

FortiGates are the foundation of the Fortinet Security Fabric—the core is FortiOS. All security and networking capabilities across the entire FortiGate platform are controlled with one intuitive operating system. FortiOS reduces complexity, costs, and response times by truly consolidating next-generation security products and services into one platform.

- A truly consolidated platform with a single OS and pane-of-glass for across the entire digital attack surface.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance.
- Leverage the latest technologies such as deception-based security.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings in addition to true TLS 1.3 support.
- Automatically prevent, detect, and mitigate advanced attacks within minutes with an integrated AI-driven security and advanced threat protection.
- Improve and unify the user experience with innovative SD-WAN capabilities with the ability to detect, contain, and isolate threats with automated segmentation.
- Utilize SPU hardware acceleration to boost network security performance.

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™ Support Services

Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East, and Asia, FortiCare offers services to meet the needs of enterprises of all sizes.

For more information, please refer to forti.net/fortiguard and forti.net/forticare

Specifications

	FORTIGATE 80F	FORTIGATE 80F-BYPASS	FORTIGATE 81F
Hardware Specifications			
GE RJ45/SFP Shared Media Pairs	2	2	2
GE RJ45 Internal Ports	8	8	8
Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)	–	1	–
USB Ports 3.0	1	1	1
Console (RJ45)	1	1	1
Internal Storage	–	–	1x 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)		4 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)		32 / 16	
Maximum Number of FortiTokens		500	
High Availability Configurations		Active / Active, Active / Passive, Clustering	
Dimensions			
Height x Width x Length (inches)		1.5 x 8.5 x 6.3	
Height x Width x Length (mm)		38.5 x 216 x 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		Dual power 12Vdc, 3A	
Power Required		Powered by 2 External DC Power Adapters, 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	

Order 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	Threat Protection
FortiCare	ASE [1]	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 Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard Industrial Service	•	•		
FortiGuard IoT Detection Service [2]	•	•		
FortiConverter Service	•	•		
IPAM Cloud [2]	•			
SD-WAN Orchestrator Entitlement [2]	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.4

FORTINET®

www.fortinet.com