

FortiGate/FortiWiFi® 40F Series

Secure SD-WAN
Next Generation Firewall



The FortiGate/FortiWiFi 40F series provides a fast 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 workflow 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

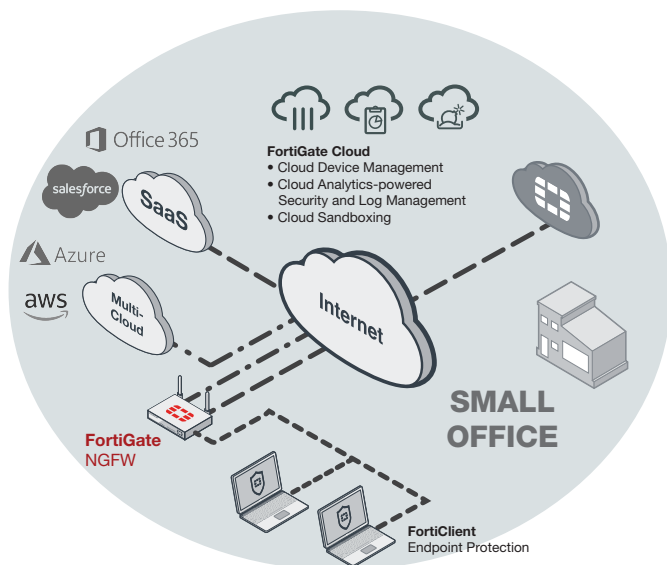
Firewall	IPS	NGFW	Threat Protection	Interfaces
5 Gbps	1 Gbps	800 Mbps	600 Mbps	Multiple GE RJ45 WiFi variants

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

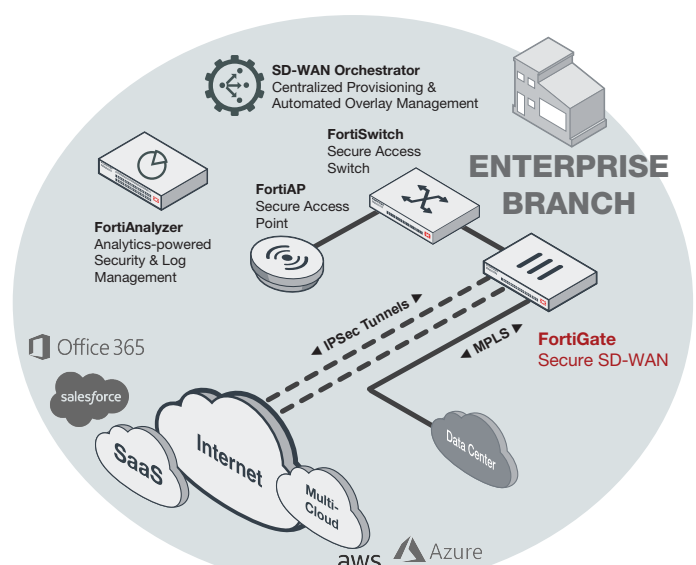


FortiWiFi 40F deployment in Small Office (NGFW)



Secure SD-WAN

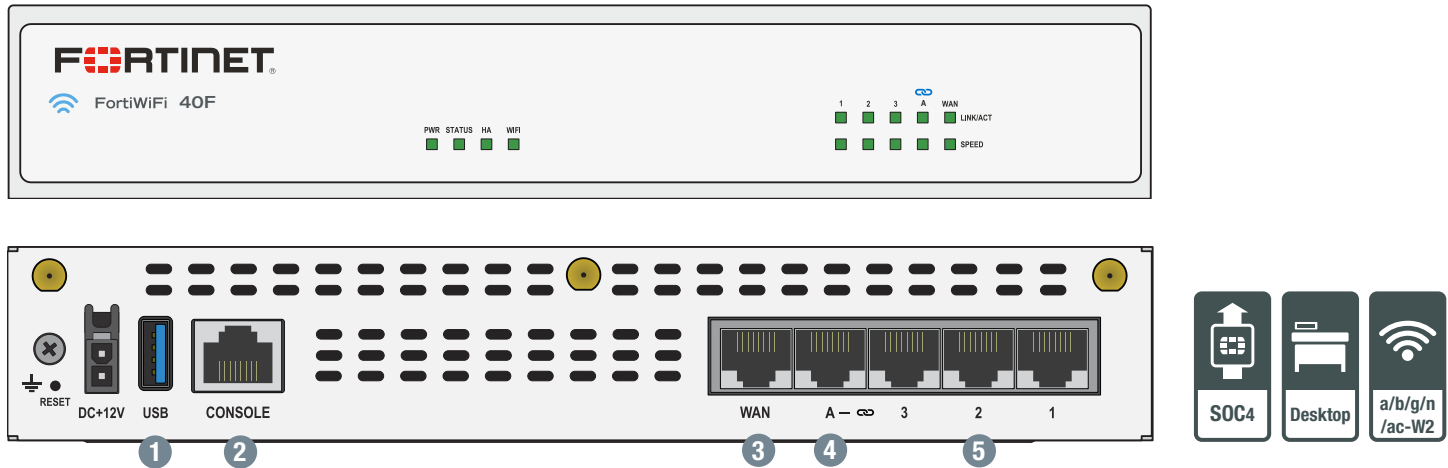
- Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport
- Accelerated Multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based 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 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 40F deployment in Enterprise Branch (Secure SD-WAN)

Hardware

FortiGate/FortiWiFi 40F Series



Interfaces

- | | |
|------------------------|------------------------------|
| 1. USB Port | 4. 1x GE RJ45 FortiLink Port |
| 2. Console Port | 5. 3x GE RJ45 Ethernet Ports |
| 3. 1x GE RJ45 WAN Port | |

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 the 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

3G/4G WAN Connectivity

The FortiGate 40F Series includes a 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 a superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Extends Security to Access Layer with FortiLink Ports

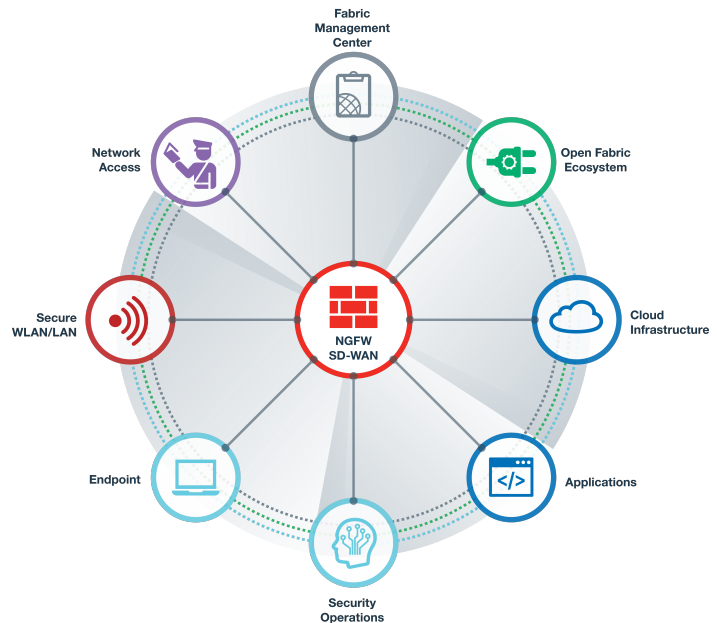
FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

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 covers 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

FortiGate is 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 40F		FORTIWIFI 40F	FORTIGATE 40F		FORTIWIFI 40F	
Hardware Specifications			Dimensions			
GE RJ45 WAN / DMZ Ports		1	Height x Width x Length (inches)			1.5 x 8.5 x 6.3
GE RJ45 Internal Ports		3	Height x Width x Length (mm)			38.5 x 216 x 160
GE RJ45 FortiLink Ports (Default)		1	Weight			2.2 lbs (1 kg)
GE RJ45 PoE/+ Ports		—	Form Factor			Desktop
Wireless Interface		—	Single Radio (2.4GHz/5GHz), 802.11/a/b/g/n/ac-W2			
USB Ports		1	Operating Environment and Certifications			
Console (RJ45)		1	Input Rating			12Vdc, 3A
Internal Storage		—	Power Required			Powered by External DC Power Adapter, 100–240V AC, 50–60 Hz
			Maximum Current			100V AC / 0.2A, 240V AC / 0.1A
System Performance — Enterprise Traffic Mix			Power Consumption (Average / Maximum)			12.4 W / 15.4 W 13.6 W / 16.6 W
IPS Throughput ²		1 Gbps	Heat Dissipation			52.55 BTU/hr 56.64 BTU/hr
NGFW Throughput ^{2,4}		800 Mbps	Operating Temperature			32–104°F (0–40°C)
Threat Protection Throughput ^{2,5}		600 Mbps	Storage Temperature			-31–158°F (-35–70°C)
			Humidity			10–90% non-condensing
System Performance			Noise Level			Fanless 0 dBA
Firewall Throughput (1518 / 512 / 64 byte UDP packets)		5/5/5 Gbps	Operating Altitude			Up to 7,400 ft (2,250 m)
Firewall Latency (64 byte UDP packets)		4 µs	Compliance			FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB
Firewall Throughput (Packets Per Second)		7.5 Mpps	Certifications			ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN
Concurrent Sessions (TCP)		700,000	Radio Specifications			
New Sessions/Second (TCP)		35,000	Multiple (MU) MIMO		—	3x3
Firewall Policies		5,000	Maximum Wi-Fi Speeds		—	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz
IPsec VPN Throughput (512 byte) ¹		4.4 Gbps	Maximum Tx Power		—	20 dBm
Gateway-to-Gateway IPsec VPN Tunnels		200	Antenna Gain		—	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz
Client-to-Gateway IPsec VPN Tunnels		250				
SSL-VPN Throughput		490 Mbps				
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		200				
SSL Inspection Throughput (IPS, avg. HTTPS) ³		310 Mbps				
SSL Inspection CPS (IPS, avg. HTTPS) ³		320				
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³		55,000				
Application Control Throughput (HTTP 64K) ²		990 Mbps				
CAPWAP Throughput (HTTP 64K)		3.5 Gbps				
Virtual Domains (Default / Maximum)		10 / 10				
Maximum Number of FortiSwitches Supported		8				
Maximum Number of FortiAPs (Total / Tunnel Mode)		16 / 8				
Maximum Number of FortiTokens		500				
High Availability Configurations		Active / Active, Active / Passive, Clustering				

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.

Order Information

Product	SKU	Description
FortiGate 40F	FG-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports)
FortiWiFi 40F	FWF-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), Wireless (802.11a/b/g/n/ac-W2)

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