

# FortiGate FortiWiFi 50G Series

FG-50G-DSL, FG-50G-SFP, FG-50G-SFP-PoE, FG-51G-SFP-POE, FWF-50G-DSL, FWF-50G-SFP



## Highlights

**Gartner Magic Quadrant Leader** for both Network Firewalls and SD-WAN.

**Security-Driven Networking** with FortiOS delivers converged networking and security.

**Unparalleled Performance** with Fortinet's patented SoC processors.

**Enterprise Security** with consolidated AI / ML-powered FortiGuard Services.

**Simplified Operations** with centralized management for networking and security, automation, deep analytics, and self-healing.

## Converged Next-Generation Firewall (NGFW) and SD-WAN

The FortiGate Next-Generation Firewall 50G series is ideal for building security-driven networks at distributed enterprise sites and transforming WAN architecture at any scale.

With a rich set of AI/ML-based FortiGuard security services and our integrated Security Fabric platform, the FortiGate FortiWiFi 50G series delivers coordinated, automated, end-to-end threat protection across all use cases.

FortiGate has the industry's first integrated SD-WAN and zero-trust network access (ZTNA) enforcement within an NGFW solution and is powered by one OS. FortiGate FortiWiFi 50G automatically controls, verifies, and facilitates user access to applications, delivering consistency with a seamless and optimized user experience.

IPS	NGFW	Threat Protection	Interfaces
2.25 Gbps	1.25 Gbps	1.1 Gbps	Multiple GE RJ45   Variants with 5G, PoE, DSL, SFP, WiFi, and/or storage



Available in



Appliance



Virtual



Hosted



Cloud



Container

## FortiOS Everywhere

### FortiOS, Fortinet's Advanced Operating System

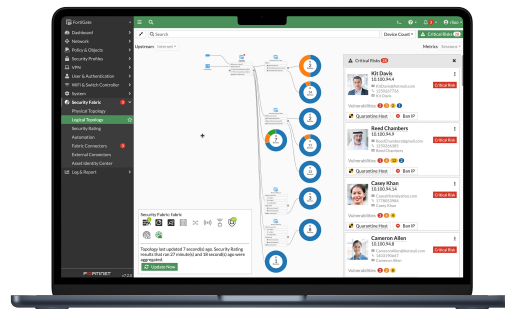
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into organically built best-of-breed capabilities, unified operating system, and ultra-scalability. The solution allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more. It provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of a simplified, single policy and management framework. Its security policies enable centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations



*Intuitive easy to use view into the network and endpoint vulnerabilities*



*Visibility with FOS Application Signatures*

### FortiConverter Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.





## FortiGuard Services

### Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

---

### Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

---

### SaaS and Data Security

SaaS and Data Security Services address numerous security use cases across application usage as well as overall data security. This service consists of Data Leak Prevention (DLP) which ensures data visibility, management, and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. The FortiGuard Data Loss Prevention Service provides advanced data protection by using real-time data classification and pattern matching to identify sensitive information. It offers comprehensive monitoring and control over data movement, ensuring that sensitive data is not inadvertently or maliciously transmitted outside the organization. Additionally, The FortiGuard Data Loss Prevention Service facilitates compliance with various regulatory requirements by automating the enforcement of data security policies and providing detailed reporting and audit trails.

---

### Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

---

### OT Security

The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.



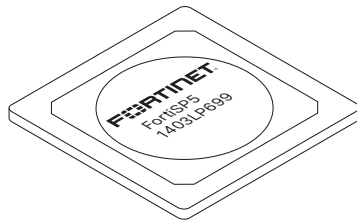
## Secure Any Edge at Any Scale



### Powered by Security Processing Unit (SPU)

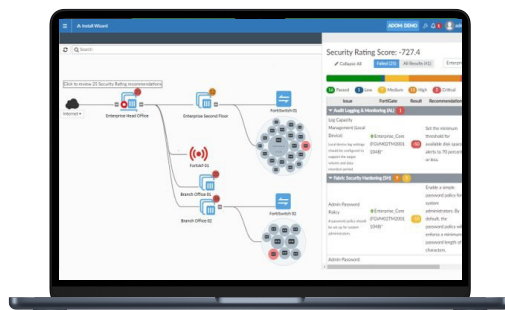
Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

### ASIC Advantage



### Secure SD-WAN ASIC SP5

- 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



*Intuitive view and clear insights into network security posture with FortiManager*

### Centralized Network and Security Management at Scale

FortiManager, the centralized management solution from Fortinet, enables integrated management of the Fortinet security fabric, including devices like FortiGate, FortiSwitch, and FortiAP. It simplifies and automates the oversight of network and security functions across diverse environments, serving as the fundamental component for deploying Hybrid Mesh Firewalls.

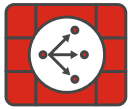


## Use Cases



### Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection



### Secure SD-WAN

- FortiGate enables best-of-breed WAN Edge with integrated SD-WAN, WAN optimization, security, and unified management from a single FortiOS operating system
- FortiGate, built on a patented SD-WAN based ASIC, delivers faster applications identification which avoids delay in accessing applications and accelerates overlay performance regardless locations
- Enhances work-from-anywhere with a comprehensive SASE solution by integrating cloud-delivered SD-WAN with Security Service Edge (SSE)
- Achieves operational efficiencies at any scale through automation, deep analytics, and self-healing



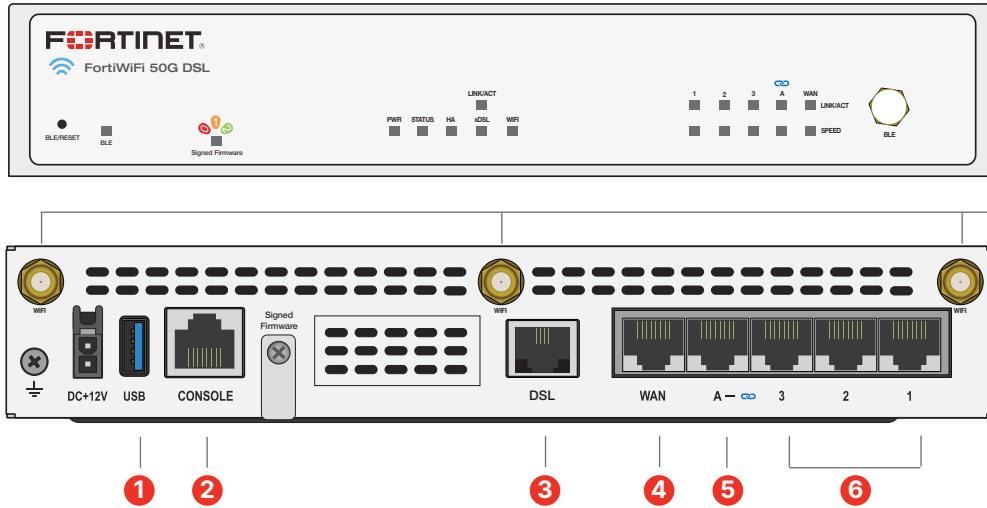
### Universal ZTNA

- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access - every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

# Hardware

## FortiGate/ FortiWiFi 50G-DSL

SP5    TPM  
 DESKTOP    GE    DSL    a/b/g/n/ac-W2/ax

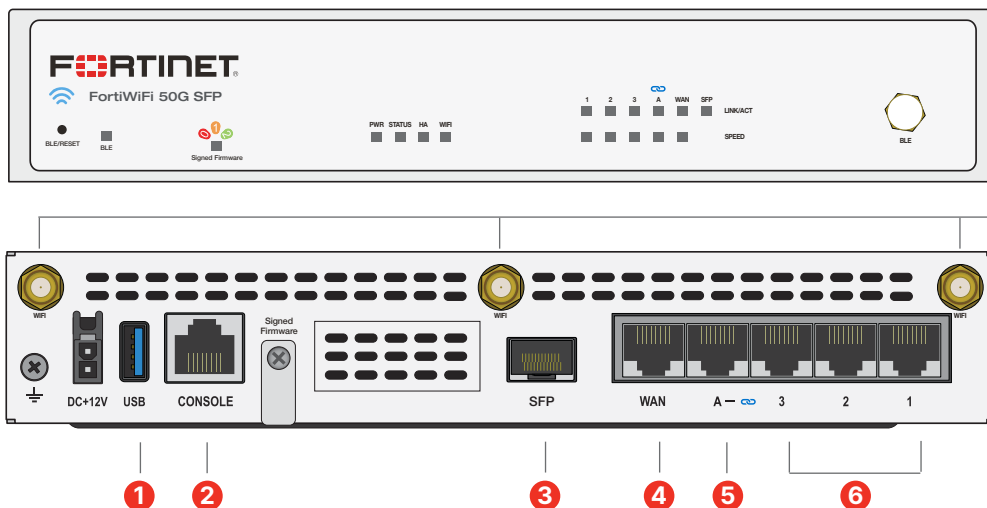


### Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 1 x DSL RJ11 Port
4. 1 x GE RJ45 WAN Port
5. 1 x GE RJ45 FortiLink Port
6. 3 x GE RJ45 Ethernet Ports
7. 3 x WiFi Antenna Ports (FWF models only)

## FortiGate/ FortiWiFi 50G-SFP

SP5    TPM  
 DESKTOP    GE    SFP    a/b/g/n/ac-W2/ax



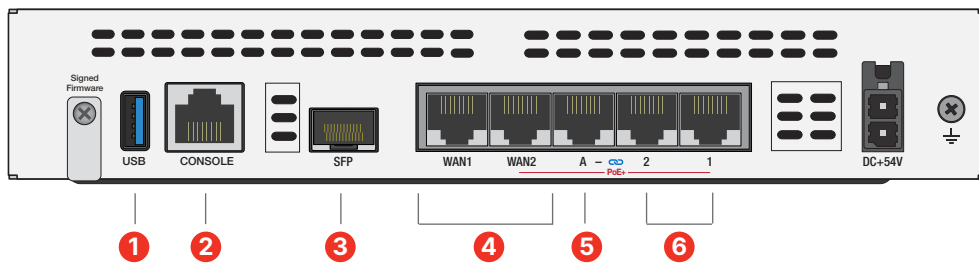
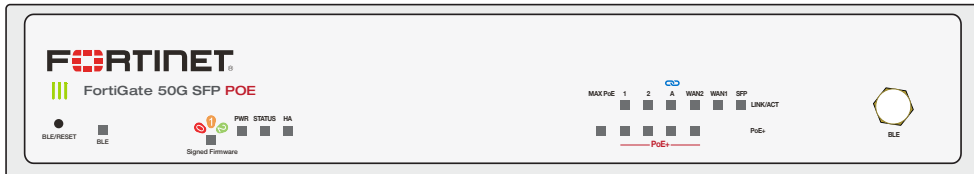
### Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 1 x GE SFP Port
4. 1 x GE RJ45 WAN Port
5. 1 x GE RJ45 FortiLink Port
6. 3 x GE RJ45 Ethernet Ports
7. 3 x WiFi Antenna Ports (FWF models only)



## Hardware

### FortiGate 50/51G-SFP-POE



### Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 1 x GE SFP Port
4. 2 x GE RJ45 WAN Ports (WAN2 PoE+)
5. 1 x GE RJ45 FortiLink Port (PoE+)
6. 2 x GE RJ45 Ethernet Ports (PoE+)

## Hardware Features



### Superior Wireless Coverage

A built-in dual-band, dual-stream access point is integrated on the FortiWiFi 50G series which provides the industry's latest high-speed WiFi-6 (802.11ax) wireless access.

---



### Trusted Platform Module (TPM)

The FortiGate FortiWiFi 50G 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.

---



### Access Layer Security

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.

---



### 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.



# Specifications

	FORTIGATE 50G-SFP	FORTIWIFI 50G-SFP	FORTIGATE 50G-SFP-POE	FORTIGATE 51G-SFP-POE
<b>Hardware Specifications</b>				
Hardware Accelerated GE WAN Ports	1	1	2	2
Hardware Accelerated GE RJ45 Ports	3	3	—	—
Hardware Accelerated GE RJ45 POE/+ Ports	—	—	4 PoE power budget 30W (802.3at)	4 PoE power budget 30W (802.3at)
Hardware Accelerated GE SFP Slots	1	1	1	1
Hardware Accelerated GE RJ45 FortiLink Port (Default)	1	1	—	—
USB Port	1	1	1	1
Console Port (RJ45)	1	1	1	1
Internal Storage	—	—	—	64 GB SSD
Trusted Platform Module (TPM)	✓	✓	✓	✓
Bluetooth Low Energy (BLE)	✓	✓	✓	✓
Antenna Ports (SMA)	—	3	—	—
Wireless Interface	—	Dual Radio (2.4 GHz/ 5 GHz), 802.11 a/b/g/n/ac/ax	—	—
<b>System Performance — Enterprise Traffic Mix</b>				
IPS Throughput <sup>2</sup>	2.25 Gbps	2.25 Gbps	2.25 Gbps	2.25 Gbps
NGFW Throughput <sup>2,4</sup>	1.25 Gbps	1.25 Gbps	1.25 Gbps	1.25 Gbps
Threat Protection Throughput <sup>2,5</sup>	1.1 Gbps	1.1 Gbps	1.1 Gbps	1.1 Gbps
<b>System Performance</b>				
Firewall Throughput (1518/512/64 byte UDP packets)	5 / 5 / 4 Gbps	5 / 5 / 4 Gbps	5 / 5 / 4 Gbps	5 / 5 / 4 Gbps
Firewall Latency (64 byte UDP packets)	2.42 μs	2.42 μs	2.42 μs	2.42 μs
Firewall Throughput (Packets Per Second)	6 Mpps	6 Mpps	6 Mpps	6 Mpps
Concurrent Sessions (TCP)	720 000	720 000	720 000	720 000
New Sessions/Second (TCP)	85 000	85 000	85 000	85 000
Firewall Policies	2000	2000	2000	2000
IPsec VPN Throughput (512 byte) <sup>1</sup>	4.5 Gbps	4.5 Gbps	4.5 Gbps	4.5 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200	200	200	200
Client-to-Gateway IPsec VPN Tunnels	250	250	250	250
SSL-VPN Throughput	—	—	—	—
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	—	—	—	—
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	1.3 Gbps	1.3 Gbps	1.3 Gbps	1.3 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	699	699	699	699
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	74 000	74 000	74 000	74 000
Application Control Throughput (HTTP 64K) <sup>2</sup>	2.8 Gbps	2.8 Gbps	2.8 Gbps	2.8 Gbps
CAPWAP Throughput (HTTP 64K)	3.8 Gbps	3.8 Gbps	3.8 Gbps	3.8 Gbps
Virtual Domains (Default/Maximum)	5/5	5/5	5/5	5/5
Maximum Number of FortiSwitches Supported	8	8	8	8
Maximum Number of FortiAPs (Total/Tunnel Mode)	16 / 8	16 / 8	16 / 8	16 / 8
Maximum Number of FortiTokens	500	500	500	500
High Availability Configurations	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering

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

<sup>1</sup> IPsec VPN performance test uses AES256-SHA256.

<sup>2</sup> IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

<sup>3</sup> SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

<sup>4</sup> NGFW performance is measured with Firewall, IPS and Application Control enabled.

<sup>5</sup> Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.



## Specifications

	FORTIGATE 50G-SFP	FORTIWIFI 50G-SFP	FORTIGATE 50G-SFP-POE	FORTIGATE 51G-SFP-POE
<b>Dimensions</b>				
Height x Width x Length (inches)	1.6 x 8.5 x 6.3	1.6 x 8.5 x 6.3	1.6 x 8.5 x 6.3	1.6 x 8.5 x 6.3
Height x Width x Length (mm)	40.5 x 216 x 160	40.5 x 216 x 160	40.5 x 216 x 160	40.5 x 216 x 160
Weight	2.2 lbs (1.0 kg)	2.2 lbs (1.0 kg)	2.2 lbs (1.0 kg)	2.2 lbs (1.0 kg)
Form Factor (supports EIA/non-EIA standards)	Desktop	Desktop	Desktop	Desktop
<b>Operating Environment and Certifications</b>				
Power Rating	12VDC, 3A	12VDC, 3A	54VDC, TBD current	54VDC, TBD current
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz
Maximum Current	100V/0.4A, 240V/0.2A	100V/0.4A, 240V/0.2A	100V/0.4A, 240V/0.2A	100V/0.4A, 240V/0.2A
Power Consumption (Average/Maximum)	8.3 W / 8.9 W	12.5 W / 13.9 W	75.4 W / 76.3 W	78.7 W / 78.1 W
Heat Dissipation	30.35 BTU/h	47.4 BTU/h	260.48 BTU/h	268.54 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	-31°F to 158°F (-35°C to 70°C)	-31°F to 158°F (-35°C to 70°C)	-31°F to 158°F (-35°C to 70°C)
Humidity	10% to 90% non-condensing	10% to 90% non-condensing	10% to 90% non-condensing	10% to 90% non-condensing
Noise Level	Fanless 0 dBA	Fanless 0 dBA	Fanless 0 dBA	Fanless 0 dBA
Operating Altitude	Up to 10 000 ft (3048 m)	Up to 10 000 ft (3048 m)	Up to 10 000 ft (3048 m)	Up to 10 000 ft (3048 m)
Compliance	FCC, ISSED, CE, UL/cUL, CB	FCC, ISSED, CE, UL/cUL, CB	FCC, IC, CE, UL/cUL, CB	FCC, IC, CE, UL/cUL, CB
Certifications	USGv6/IPv6	USGv6/IPv6	USGv6/IPv6	USGv6/IPv6
<b>Radio Specifications</b>				
Multiple User (MU) MIMO	—	2 x 2	—	—
Maximum Wi-Fi Speeds	—	1201 Mbps @ 5 GHz, 574 Mbps @ 2.4 GHz	—	—
Maximum Tx Power	—	21.0 dBm per chain @ 2.4GHz, 19.5 dBm per chain @ 5GHz	—	—



# Specifications

	FORTIGATE 50G-DSL	FORTIWIFI 50G-DSL
<b>Hardware Specifications</b>		
Hardware Accelerated GE WAN Ports	1	1
Hardware Accelerated GE RJ45 Ports	3	3
Hardware Accelerated GE RJ45 FortiLink Ports (Default)	1	1
DSL RJ11 Port	1	1
USB Port	1	1
Console Port (RJ45)	1	1
Trusted Platform Module (TPM)	☑	☑
Bluetooth Low Energy (BLE)	☑	☑
Antenna Ports (SMA)	—	3
Wireless Interface	—	Dual Radio (2.4 GHz/ 5 GHz), 802.11 a/b/g/n/ac/ax
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>	2.25 Gbps	2.25 Gbps
NGFW Throughput <sup>2,4</sup>	1.25 Gbps	1.25 Gbps
Threat Protection Throughput <sup>2,5</sup>	1.1 Gbps	1.1 Gbps
<b>System Performance</b>		
Firewall Throughput (1518/512/64 byte UDP packets)	5 / 5 / 4 Gbps	5 / 5 / 4 Gbps
Firewall Latency (64 byte UDP packets)	2.42 μs	2.42 μs
Firewall Throughput (Packets Per Second)	6 Mpps	6 Mpps
Concurrent Sessions (TCP)	720 000	720 000
New Sessions/Second (TCP)	85 000	85 000
Firewall Policies	2000	2000
IPsec VPN Throughput (512 byte) <sup>1</sup>	4.5 Gbps	4.5 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200	200
Client-to-Gateway IPsec VPN Tunnels	250	250
SSL-VPN Throughput	—	—
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	—	—
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	1.3 Gbps	1.3 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	699	699
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	74 000	74 000
Application Control Throughput (HTTP 64K) <sup>2</sup>	2.8 Gbps	2.8 Gbps
CAPWAP Throughput (HTTP 64K)	3.8 Gbps	3.8 Gbps
Virtual Domains (Default/Maximum)	5/5	5/5
Maximum Number of FortiSwitches Supported	8	8
Maximum Number of FortiAPs (Total/Tunnel Mode)	16 / 8	16 / 8
Maximum Number of FortiTokens	500	500
High Availability Configurations	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering

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

<sup>1</sup> IPsec VPN performance test uses AES256-SHA256.

<sup>2</sup> IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

<sup>3</sup> SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

<sup>4</sup> NGFW performance is measured with Firewall, IPS and Application Control enabled.

<sup>5</sup> Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.



# Specifications

	FORTIGATE 50G-DSL	FORTIWIFI 50G-DSL
<b>Dimensions</b>		
Height x Width x Length (inches)	1.7 x 8.5 x 7.0	1.7 x 8.5 x 7.0
Height x Width x Length (mm)	42 x 216 x 178	42 x 216 x 178
Weight	2.2 lbs (1.0 kg)	2.2 lbs (1.0 kg)
Form Factor (supports EIA/non-EIA standards)	Desktop	Desktop
<b>Operating Environment and Certifications</b>		
Power Rating	12VDC, 3A	12VDC, 3A
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz
Maximum Current	100V/0.2A, 240V/0.1A	100V/0.3A, 240V/0.15A
Power Consumption (Average/Maximum)	12.43 W / 13.01 W	17.74 W / 19.0 W
Heat Dissipation	44.36 BTU/hr	64.79 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	-31°F to 158°F (-35°C to 70°C)
Humidity	10% to 90% non-condensing	10% to 90% non-condensing
Noise Level	Fanless 0 dBA	Fanless 0 dBA
Operating Altitude	Up to 10 000 ft (3048 m)	Up to 10 000 ft (3048 m)
Compliance	FCC, ISSED, CE, UL/cUL, CB	FCC, ISSED, CE, UL/cUL, CB
Certifications	USGv6/IPv6	USGv6/IPv6
<b>xDSL Modem Supported Mode</b>		
vDSL2	☑	☑
ADSL2	☑	☑
ADSL2+	☑	☑
G.DMT	☑	☑
T1.413	☑	☑
G.Lite	☑	☑
<b>xDSL Modem Supported Type</b>		
Annex A, B, I, J, M, L	☑	☑
<b>Radio Specifications</b>		
Multiple User (MU) MIMO	—	2 x 2
Maximum Wi-Fi Speeds	—	1201 Mbps @ 5 GHz, 574 Mbps @ 2.4 GHz
Maximum Tx Power	—	21.0 dBm per chain @ 2.4GHz, 19.5 dBm per chain @ 5GHz



## Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct <sup>3</sup> , AI-based Heuristic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video <sup>3</sup> Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention <sup>3</sup>	•	•		
	Data Loss Prevention (DLP) <sup>1</sup>	•	•		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	•	•		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS <sup>1</sup>	•			
	Application Control			included with FortiCare Subscription	
	Inline CASB <sup>3</sup>		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring	•			
	SD-WAN Overlay-as-a-Service	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth) <sup>2</sup>	•			
NOC and SOC Services	FortiConverter Service for one time configuration conversion	•	•		
	Managed FortiGate Service—available 24×7, with Fortinet NOC experts performing device setup, network, and policy change management	•			
	FortiGate Cloud—Management, Analysis, and One Year Log Retention	•			
	FortiManager Cloud	•			
	FortiAnalyzer Cloud	•			
	FortiGuard SOCaas—24×7 cloud-based managed log monitoring, incident triage, and SOC escalation service	•			
Hardware and Software Support	FortiCare Essentials <sup>2</sup>	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Device/OS Detection, GeolPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing		included with FortiCare Subscription		

1. Full features available when running FortiOS 7.4.1.

2. Desktop Models only.

3. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 50G series in any OS build.



### FortiGuard Bundles

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.



### FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive lifecycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service variants, offers heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an Extended End-of-Engineering-Support of 18 months, providing flexibility. Access the intuitive FortiCare Elite Portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.



## Ordering Information

Product	SKU	Description
FortiGate 50G-DSL	FG-50G-DSL	5x GE RJ45 ports (including 4x Internal Ports, 1x WAN Ports) with 1x embeded DSL module.
FortiGate 50G-SFP	FG-50G-SFP	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), 1x SFP port.
FortiGate 50G-SFP-POE	FG-50G-SFP-PoE	3x RJ45 PoE+ ports, 1x RJ45 PoE+ WAN, 1 x RJ45 WAN port, 1x SFP port.
FortiGate-51G-SFP-PoE	FG-51G-SFP-POE	3x RJ45 PoE+ ports, 1x RJ45 PoE+ WAN, 1x RJ45 WAN port, 1x SFP port, with 64GB SSD storage.
FortiWiFi 50G-DSL	FWF-50G-DSL-[RC]	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), 1x DSL port, Wireless (802.11a/b/g/n/ac/ax).
FortiWiFi 50G-SFP	FWF-50G-SFP-[RC]	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), 1x SFP, Wireless (802.11a/b/g/n/ac/ax).
<b>Optional Accessories</b>		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E, F, and G series desktop models are backwards compatible with SP-RackTray-01.
Mounting Ear Bracket	SP-EAR-FG90G-10	Mounting Ear brackets for FWF-50G series and FG-90/91G 10 pairs pack.
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-50G series, FG/FWF-60F series , and FG/FWF-80F series.
AC Power Adaptor	SP-FG-40F-PA-10(-XX)	Pack of 10 AC power adaptors for FWF-50G series and FG/FWF-40F, come with interchangeable power plugs. (XX=various countries code).
	SP-FG50G-POE-PDC-5	Pack of 5 AC power adaptors for FG-50/51G-SFP-POE, power cable SP-FGPCOR-XX sold separately.

[RC] = regional code: A, B, D, E, F, I, J, N, P, S, V, and Y

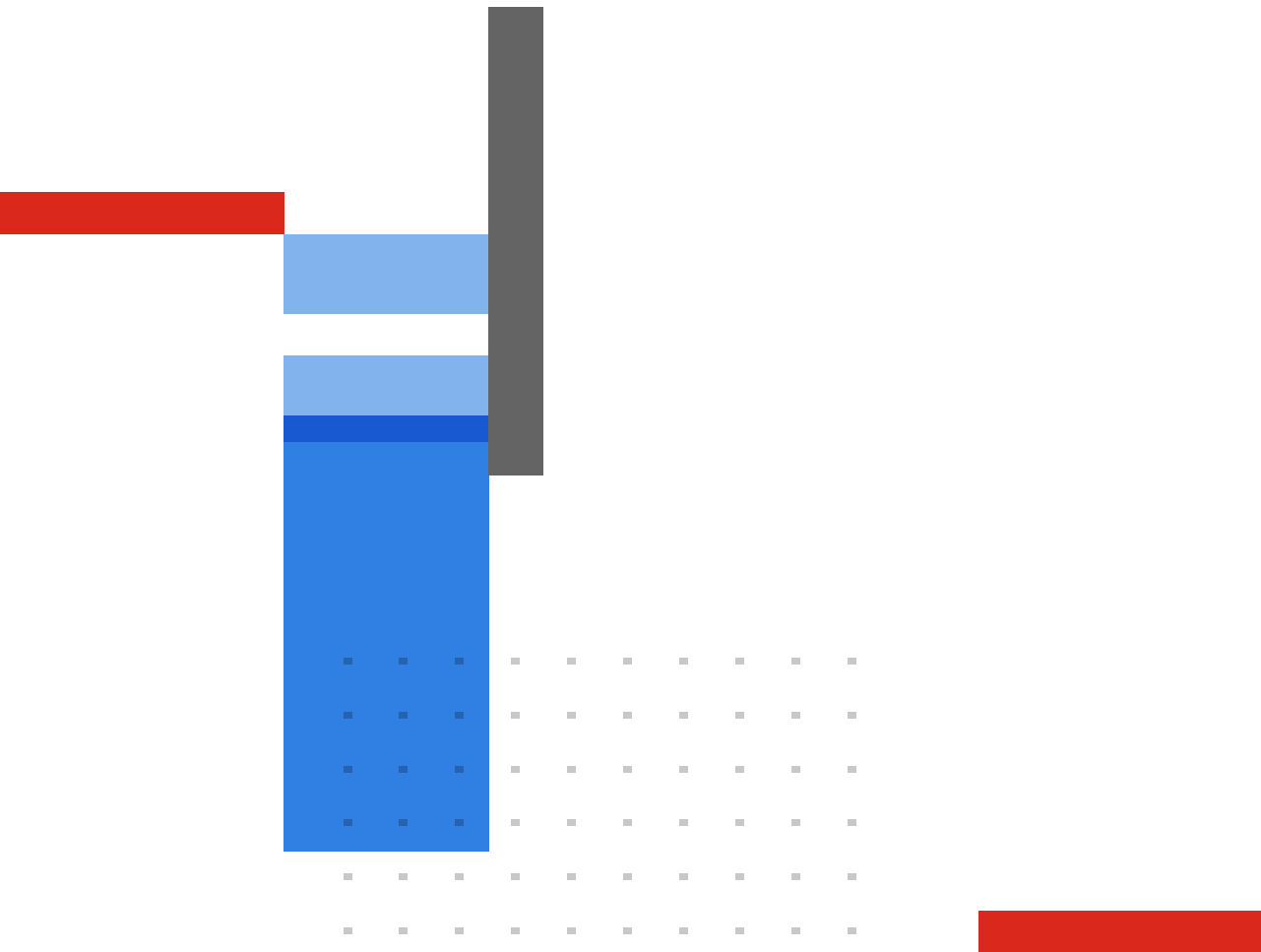
Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.



---

## Fortinet Corporate Social Responsibility Policy

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](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2024 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 SVP Legal and above, 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.