

# FortiGate/FortiWiFi® 50E Series

FG-50E, FG-51E, FWF-50E, and FWF-51E

Secure SD-WAN  
Next Generation Firewall



The FortiGate/FortiWiFi 50E 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  |
|----------|----------|----------|-------------------|---|
| 2.5 Gbps | 350 Mbps | 220 Mbps | 160 Mbps          | Multiple GE RJ45   WiFi variants   Variants with internal storage |

## DEPLOYMENT



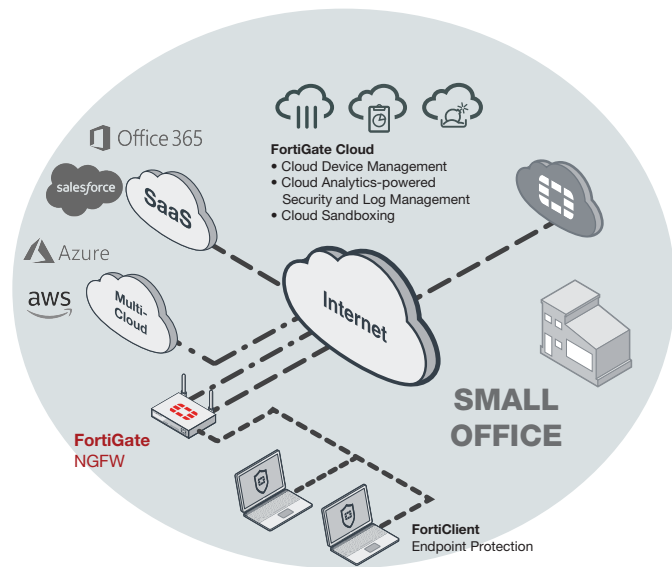
### Next Generation Firewall (NGFW)

- 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

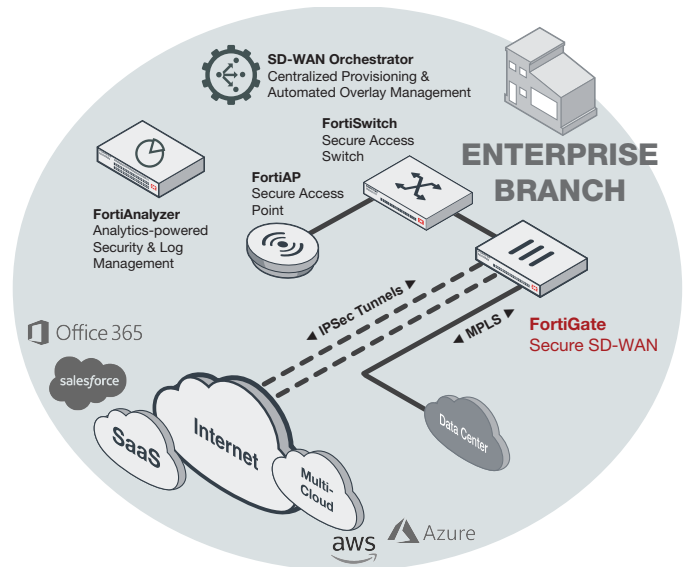


### Secure SD-WAN

- 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



Next Generation Firewall Small Office Deployment

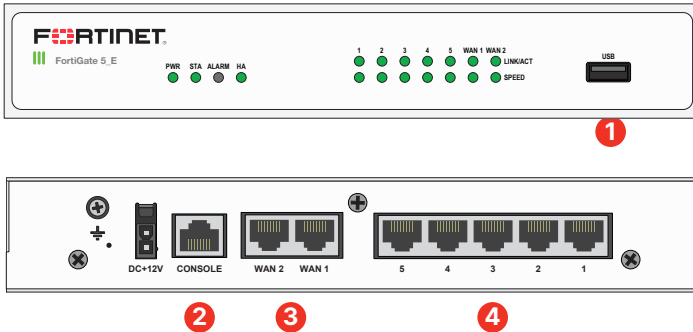


Secure SD-WAN Enterprise Branch Deployment



## HARDWARE

### FortiGate 50E/51E



### Hardware Features



### Interfaces

1. 1x USB Port
2. 1x Console RJ45
3. 2x GE RJ45 WAN Ports
4. 5x GE RJ45 Switch Ports

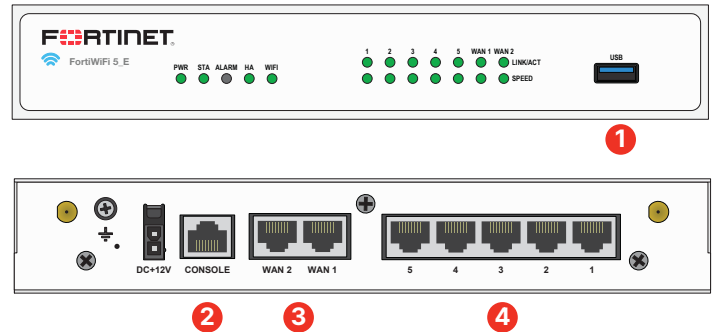
### Install in Minutes with FortiExplorer

The FortiExplorer wizard enables easy setup and configuration coupled with easy-to-follow instructions. FortiExplorer runs on popular iOS devices. Using FortiExplorer is as simple as starting the application and connecting to the appropriate USB port on the FortiGate. By using FortiExplorer, you can be up and running and protected in minutes.

### Wireless and 3G/4G WAN Extensions

The FortiGate supports external 3G/4G modems that allow additional or redundant WAN connectivity for maximum reliability. The FortiGate can also operate as a wireless access point controller to further extend wireless capabilities.

### FortiWiFi 50E/51E



### Hardware Features



### Interfaces

1. 1x USB Port
2. 1x Console RJ45
3. 2x GE RJ45 WAN Ports
4. 5x GE RJ45 Switch Ports

### Compact and Reliable Form Factor

Designed for small environments, you can simply place the FortiGate/FortiWiFi 50E series on a desktop. It is small, lightweight yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

### Superior Wireless Coverage

A built-in dual-band, dual-stream access point with internal antennas is integrated on the FortiWiFi 50E and provides speedy 802.11ac wireless access. The dual-band chipset addresses the PCI-DSS compliance requirement for rogue AP wireless scanning, providing maximum protection for regulated environments.

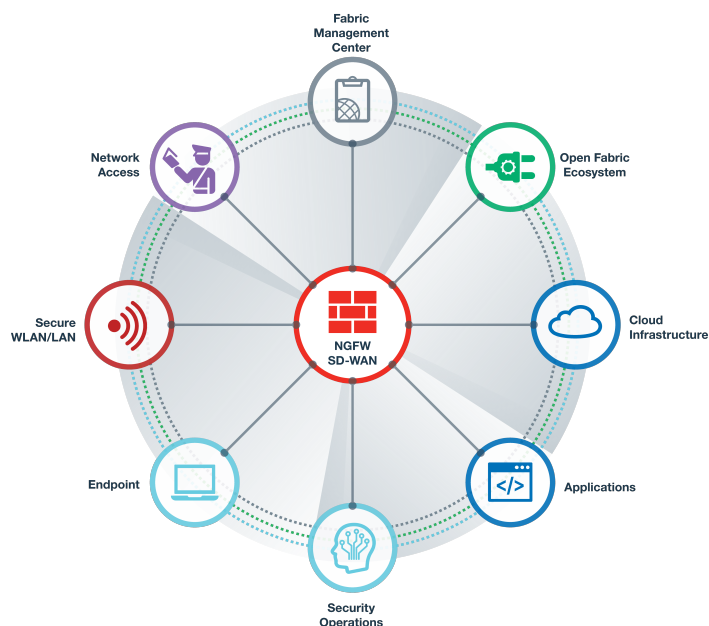


## FORTINET SECURITY FABRIC

### 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

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](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)



# SPECIFICATIONS

|  | FG-50E                  | FWF-50E                            | FG-51E                                    | FWF-51E                            |
|--|-------------------------|------------------------------------|---|------------------------------------|
| <b>Hardware Specifications</b>                                   |                         |                                    |   |                                    |
| GE RJ45 Switch Ports   |                         |                                    | 5   |                                    |
| GE RJ45 WAN Ports  |                         |                                    | 2   |                                    |
| USB Ports  |                         |                                    | 1   |                                    |
| Console (RJ45)   |                         |                                    | 1   |                                    |
| Wireless Interface   | —                       | 802.11 a/b/g/n                     | —   | 802.11 a/b/g/n                     |
| Internal Storage   | —                       | —                                  | 1× 32 GB SSD                              | 1× 32 GB SSD                       |
| <b>System Performance — Enterprise Traffic Mix</b>               |                         |                                    |   |                                    |
| IPS Throughput <sup>2</sup>                                      |                         |                                    | 350 Mbps                                  |                                    |
| NGFW Throughput <sup>2,4</sup>                                   |                         |                                    | 220 Mbps                                  |                                    |
| Threat Protection Throughput <sup>2,5</sup>                      |                         |                                    | 160 Mbps                                  |                                    |
| <b>System Performance</b>  |                         |                                    |   |                                    |
| Firewall Throughput  |                         |                                    | 2.5 Gbps                                  |                                    |
| Firewall Latency (64 byte UDP packets)                           |                         |                                    | 180 μs                                    |                                    |
| Firewall Throughput (Packets Per Second)                         |                         |                                    | 375 Kpps                                  |                                    |
| Concurrent Sessions (TCP)  |                         |                                    | 1.8 Million                               |                                    |
| New Sessions/Second (TCP)  |                         |                                    | 21,000                                    |                                    |
| Firewall Policies  |                         |                                    | 5,000                                     |                                    |
| IPsec VPN Throughput (512 byte) <sup>1</sup>                     |                         |                                    | 90 Mbps                                   |                                    |
| Gateway-to-Gateway IPsec VPN Tunnels                             |                         |                                    | 200                                       |                                    |
| Client-to-Gateway IPsec VPN Tunnels                              |                         |                                    | 250                                       |                                    |
| SSL-VPN Throughput   |                         |                                    | 100 Mbps                                  |                                    |
| Concurrent SSL-VPN Users<br>(Recommended Maximum, Tunnel Mode)   |                         |                                    | 200                                       |                                    |
| SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>         |                         |                                    | 150 Mbps                                  |                                    |
| SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>                |                         |                                    | 140                                       |                                    |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup> |                         |                                    | 75,000                                    |                                    |
| Application Control Throughput (HTTP 64K) <sup>2</sup>           |                         |                                    | 450 Mbps                                  |                                    |
| CAPWAP Throughput (HTTP 64K)                                     |                         |                                    | 1.2 Gbps                                  |                                    |
| Virtual Domains (Default / Maximum)                              |                         |                                    | 5 / 5                                     |                                    |
| Maximum Number of FortiSwitches Supported                        |                         |                                    | 8   |                                    |
| Maximum Number of FortiAPs (Total / Tunnel Mode)                 |                         |                                    | 10 / 5                                    |                                    |
| Maximum Number of FortiTokens                                    |                         |                                    | 500                                       |                                    |
| High Availability Configurations                                 |                         |                                    | Active/Active, Active/Passive, Clustering |                                    |
| <b>Dimensions</b>  |                         |                                    |   |                                    |
| Height x Width x Length (inches)                                 |                         |                                    | 1.44 × 8.52 × 5.5                         |                                    |
| Height x Width x Length (mm)                                     |                         |                                    | 36.5 × 216 × 140                          |                                    |
| Weight   | 2.015 lbs<br>(0.914 kg) | 2.041 lbs<br>(0.926 kg)            | 2.04 lbs<br>(0.925 kg)                    | 2.04 lbs<br>(0.925 kg)             |
| Form Factor  |                         |                                    | Desktop                                   |                                    |
| <b>Radio Specifications</b>                                      |                         |                                    |   |                                    |
| MIMO   | —                       | 2×2                                | —   | 2×2                                |
| Maximum Wi-Fi Speeds   | —                       | 300 Mbps                           | —   | 300 Mbps                           |
| Maximum Tx Power   | —                       | 21 dBm                             | —   | 21 dBm                             |
| Antenna Gain   | —                       | 2 dBi @ 5 GHz,<br>2.4dBi @ 2.4 GHz | —   | 2 dBi @ 5 GHz,<br>2.4dBi @ 2.4 GHz |

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.



# SPECIFICATIONS

|   | FG-50E  | FWF-50E   | FG-51E    | FWF-51E   |
|---|---|-----------|-----------|-----------|
| <b>Operating Environment and Certifications</b> |   |           |           |           |
| <b>Input Rating</b>                             | 12Vdc, 2A   |           |           |           |
| <b>Power Required</b>                           | Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz |           |           |           |
| <b>Maximum Current</b>                          | 100 V / 0.6 A, 240 V / 0.4 A                                |           |           |           |
| <b>Power Consumption (Average / Maximum)</b>    | 15 / 18 W   | 18 / 22 W | 16 / 20 W | 19 / 23 W |
| <b>Heat Dissipation</b>                         | 62 BTU/h  | 75 BTU/h  | 67 BTU/h  | 79 BTU/h  |
| <b>Operating Temperature</b>                    | 32–104°F (0–40°C)   |           |           |           |
| <b>Storage Temperature</b>                      | -31–158°F (-35–70°C)  |           |           |           |
| <b>Humidity</b>                                 | 10–90% non-condensing                                       |           |           |           |
| <b>Noise Level</b>                              | Fanless 0 dBA   |           |           |           |
| <b>Operating Altitude</b>                       | Up to 7,400 ft (2,250 m)                                    |           |           |           |
| <b>Regulatory Compliance</b>                    | FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB                  |           |           |           |
| <b>Certifications</b>                           | ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN         |           |           |           |

# ORDERING INFORMATION

| Product                   | SKU            | Description   |
|---------------------------|----------------|---|
| <b>FortiGate 50E</b>      | FG-50E         | 7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports)  |
| <b>FortiWiFi 50E</b>      | FWF-50E        | 7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports), Wireless (802.11a/b/g/n)  |
| <b>FortiGate 51E</b>      | FG-51E         | 7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports), 32 GB SSD onboard storage   |
| <b>FortiWiFi 51E</b>      | FWF-51E        | 7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports), Wireless (802.11a/b/g/n), 32 GB SSD onboard storage                                   |
| <b>Optional Accessory</b> |                |   |
| <b>Rack Mount Tray</b>    | SP-RACKTRAY-02 | Rack mount tray for FG-30D, FG-40C, FG-50/51E, FG-60C, FG-60D/-POE, FG-70D, FG-80D, FG-90D/-POE, FAD-100E, FRC-100D, FWB-100D, FML-60D, FVE-100E. |

# 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 | SMB Protection | Unified Threat Protection | Advanced Threat Protection |
|--|-----------------------|----------------|---------------------------|----------------------------|
| <b>FortiCare</b>   | 24x7                  | 24x7           | 24x7                      | 24x7                       |
| <b>FortiGuard App Control Service</b>  | •                     | •              | •                         | •                          |
| <b>FortiGuard IPS Service</b>  | •                     | •              | •                         | •                          |
| <b>FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service</b> | •                     | •              | •                         | •                          |
| <b>FortiGuard Web and Video<sup>1</sup> Filtering Service</b>  | •                     | •              | •                         |                            |
| <b>FortiGuard Antispam Service</b>   | •                     | •              | •                         |                            |
| <b>FortiGuard Security Rating Service</b>  | •                     |                |                           |                            |
| <b>FortiGuard IoT Detection Service</b>  | •                     |                |                           |                            |
| <b>FortiGuard Industrial Service</b>   | •                     |                |                           |                            |
| <b>FortiConverter Service</b>  | •                     |                |                           |                            |
| <b>FortiGate Cloud Subscription</b>  |                       | •              |                           |                            |

1. 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.