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 (VDOMs) 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

### Specifications

<table>
<thead>
<tr>
<th>Firewall</th>
<th>IPS</th>
<th>NGFW</th>
<th>Threat Protection</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5 Gbps</td>
<td>350 Mbps</td>
<td>220 Mbps</td>
<td>160 Mbps</td>
<td>Multiple GE RJ45</td>
</tr>
</tbody>
</table>
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
**HARDWARE**

**FortiGate 50E/51E**

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

**FortiWiFi 50E/51E**

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

**Hardware Features**

- Desktop
- 32GB
- 64GB

**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.

**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 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

<table>
<thead>
<tr>
<th>Hardware Specifications</th>
<th>FG-50E</th>
<th>FWF-50E</th>
<th>FG-51E</th>
<th>FWF-51E</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE RJ45 Switch Ports</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GE RJ45 WAN Ports</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USB Ports</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Console (RJ45)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Interface</td>
<td>802.11 a/b/g/n</td>
<td>802.11 a/b/g/n</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Storage</td>
<td>—</td>
<td>—</td>
<td>1x 32 GB SSD</td>
<td>1x 32 GB SSD</td>
</tr>
</tbody>
</table>

### System Performance — Enterprise Traffic Mix

**IPS Throughput**

- 350 Mbps

**NGFW Throughput**

- 220 Mbps

**Threat Protection Throughput**

- 160 Mbps

### System Performance

**Firewall Throughput**

- 2.5 Gbps

**Firewall Latency (64 byte UDP packets)**

- 180 μs

**Concurrent Sessions (TCP)**

- 1.8 Million

**New Sessions/Second (TCP)**

- 21,000

**Firewall Policies**

- 5,000

**IPsec VPN Throughput (512 byte)**

- 90 Mbps

**Gateway-to-Gateway IPsec VPN Tunnels**

- 200

**SSL-VPN Throughput**

- 450 Mbps

**Concurrent SSL-VPN Users**

- 200

**SSL Inspection Throughput (IPS, avg. HTTPS)**

- 150 Mbps

### Application Control Throughput (HTTP 64K)

- 600 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

### Dimensions

| Height x Width x Length (inches) | 1.44 x 8.52 x 5.5 |
| Height x Width x Length (mm)    | 36.5 x 216 x 140 |

**Weight**

<table>
<thead>
<tr>
<th>FG-50E</th>
<th>FWF-50E</th>
<th>FG-51E</th>
<th>FWF-51E</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.015 lbs (0.914 kg)</td>
<td>2.041 lbs (0.926 kg)</td>
<td>2.04 lbs (0.925 kg)</td>
<td>2.04 lbs (0.925 kg)</td>
</tr>
</tbody>
</table>

### Form Factor

- Desktop

### Radio Specifications

<table>
<thead>
<tr>
<th>MIMO</th>
<th>FG-50E</th>
<th>FWF-50E</th>
<th>FG-51E</th>
<th>FWF-51E</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2×2</td>
<td>2×2</td>
<td>2×2</td>
<td>2×2</td>
</tr>
</tbody>
</table>

**Maximum Wi-Fi Speeds**

- 300 Mbps

**Maximum Tx Power**

- 21 dbm

**Antenna Gain**

- 2 dBi @ 5 GHz, 2.4 dBi @ 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

<table>
<thead>
<tr>
<th>FG-50E</th>
<th>FWF-50E</th>
<th>FG-51E</th>
<th>FWF-51E</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input Rating</strong></td>
<td>12Vdc, 2A</td>
<td><strong>Input Rating</strong></td>
<td>Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz</td>
</tr>
<tr>
<td><strong>Power Required</strong></td>
<td>100 V / 0.6 A, 240 V / 0.4 A</td>
<td><strong>Power Required</strong></td>
<td>100 V / 0.6 A, 240 V / 0.4 A</td>
</tr>
<tr>
<td><strong>Power Consumption (Average / Maximum)</strong></td>
<td>15 / 18 W</td>
<td><strong>Power Consumption (Average / Maximum)</strong></td>
<td>18 / 22 W</td>
</tr>
<tr>
<td><strong>Heat Dissipation</strong></td>
<td>62 BTU/h</td>
<td><strong>Heat Dissipation</strong></td>
<td>75 BTU/h</td>
</tr>
<tr>
<td><strong>Operating Temperature</strong></td>
<td>32–104°F (0–40°C)</td>
<td><strong>Operating Temperature</strong></td>
<td>32–104°F (0–40°C)</td>
</tr>
<tr>
<td><strong>Storage Temperature</strong></td>
<td>Up to 7,400 ft (2,250 m)</td>
<td><strong>Storage Temperature</strong></td>
<td>Up to 7,400 ft (2,250 m)</td>
</tr>
<tr>
<td><strong>Humidity</strong></td>
<td>10–90% non-condensing</td>
<td><strong>Humidity</strong></td>
<td>10–90% non-condensing</td>
</tr>
<tr>
<td><strong>Regulatory Compliance</strong></td>
<td>FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB</td>
<td><strong>Regulatory Compliance</strong></td>
<td>ICSA Labs: Firewall, IPS, IPS, Antivirus, SSL-VPN</td>
</tr>
<tr>
<td><strong>Certifications</strong></td>
<td>FortiGate 50E</td>
<td><strong>Certifications</strong></td>
<td>FortiGate 51E</td>
</tr>
</tbody>
</table>

### ORDERING INFORMATION

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 50E</td>
<td>FG-50E</td>
<td>7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports)</td>
</tr>
<tr>
<td>FortiWiFi 50E</td>
<td>FWF-50E</td>
<td>7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports), Wireless (802.11a/b/g/n)</td>
</tr>
<tr>
<td>FortiGate 51E</td>
<td>FG-51E</td>
<td>7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports), 32 GB SSD onboard storage</td>
</tr>
<tr>
<td>FortiWiFi 51E</td>
<td>FWF-51E</td>
<td>7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports), Wireless (802.11a/b/g/n), 32 GB SSD onboard storage</td>
</tr>
</tbody>
</table>

**Optional Accessory**

| Rack Mount Tray | 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 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.

<table>
<thead>
<tr>
<th>Bundles</th>
<th>360 Protection</th>
<th>Enterprise Protection</th>
<th>UTM</th>
<th>Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</td>
<td>ASE 1</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
<tr>
<td>FortiGuard App Control Service</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
<tr>
<td>FortiGuard IPS Service</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
<tr>
<td>FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
<tr>
<td>FortiGuard Web Filtering Service</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
<tr>
<td>FortiGuard Security Rating Service</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
<tr>
<td>FortiGuard Industrial Service</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
<tr>
<td>FortiCASB SaaS-only Service</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
<tr>
<td>FortiConverter Service</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
<tr>
<td>SD-WAN Cloud Assisted Monitoring 2</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
<tr>
<td>SD-WAN Overlay Controller VPN Service</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
<tr>
<td>FortiAnalyzer Cloud</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
<tr>
<td>FortiManager Cloud 2</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td></td>
</tr>
</tbody>
</table>

1. 24x7 plus Advanced Services Ticket Handling
2. Available when running FortiOS 6.2

**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.