The FortiGate/FortiWiFi 60F 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

**Networking**
- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

**Management**
- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- 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

### 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>10 Gbps</td>
<td>1.4 Gbps</td>
<td>1 Gbps</td>
<td>700 Mbps</td>
<td>Multiple GE RJ45</td>
</tr>
</tbody>
</table>

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 and optimization
- Multi-cloud access for faster SaaS adoption with end-to-end optimization
- Simplification with zero touch deployment and centralized management with auto-provisioning, analytics and reporting
- Strong security posture with next generation firewall and real-time threat protection

---

**FortiGate 60F deployment in Small Office (NGFW)**

- **FortiGate NGFW**
- **FortiAnalyzer Analytics-powered Security & Log Management**
- **FortiSwitch Secure Access Switch**
- **FortiManager Automation-Driven Network Management**
- **FortiSwitch Secure Access Switch**

**FortiWiFi 60F deployment in Small Office (NGFW)**

- **FortiWiFi 60F**
- **FortiClient Endpoint Protection**
- **FortiManager Cloud Device Management**
- **FortiManager Cloud Analytics-powered Security and Log Management**
- **FortiManager Cloud Sandboxing**

**FortiGate 60F deployment in Enterprise Branch (Secure SD-WAN)**

- **FortiGate Secure SD-WAN**
- **FortiAnalyzer Analytics-powered Security & Log Management**
- **FortiSwitch Secure Access Switch**
- **FortiManager Automation-Driven Network Management**
- **FortiSwitch Secure Access Switch**

---

**FortiManager Cloud Device Management**

- **FortiManager Cloud Analytics-powered Security and Log Management**
- **FortiManager Cloud Sandboxing**
Hardware

FortiGate/FortiWiFi 60F/61F

3G/4G WAN Connectivity
The FortiGate 60F 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 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.

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 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

Interfaces
1. USB Port
2. Console Port
3. 2x GE RJ45 WAN Ports
4. 1x GE RJ45 DMZ Port
5. 2x GE RJ45 FortiLink Ports
6. 5x GE RJ45 Internal Ports

3G/4G WAN Connectivity
The FortiGate 60F 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 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 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

<table>
<thead>
<tr>
<th>Hardware Specifications</th>
<th>FORTIGATE 60F</th>
<th>FORTIGATE 61F</th>
<th>FORTIWIFI 60F</th>
<th>FORTIWIFI 61F</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE RJ45 WAN / DMZ Ports</td>
<td>2 / 1</td>
<td>2 / 1</td>
<td>2 / 1</td>
<td>2 / 1</td>
</tr>
<tr>
<td>GE RJ45 Internal Ports</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>GE RJ45 FortiLink Ports</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Wireless Interface</td>
<td>–</td>
<td>–</td>
<td>802.11 a/b/g/n-ac-W2</td>
<td>802.11 a/b/g/n-ac-W2</td>
</tr>
<tr>
<td>USB Ports</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Console (RJ45)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Internal Storage</td>
<td>–</td>
<td>1 x 128 GB SSD</td>
<td>–</td>
<td>1 x 128 GB SSD</td>
</tr>
</tbody>
</table>

### System Performance — Enterprise Traffic Mix

<table>
<thead>
<tr>
<th>Performance Category</th>
<th>FORTIWIFI 60F</th>
<th>FORTIWIFI 61F</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Throughput</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>NGFW Throughput</td>
<td>700 Mbps</td>
<td>700 Mbps</td>
</tr>
<tr>
<td>Threat Protection Throughput</td>
<td>700 Mcps</td>
<td>700 Mcps</td>
</tr>
</tbody>
</table>

### System Performance

<table>
<thead>
<tr>
<th>Performance Category</th>
<th>FORTIWIFI 60F</th>
<th>FORTIWIFI 61F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput</td>
<td>10 Gbps</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>Firewalls Throughput</td>
<td>10/10/6 Gbps</td>
<td>10/10/6 Gbps</td>
</tr>
<tr>
<td>Firewall Latency</td>
<td>4 μs</td>
<td>4 μs</td>
</tr>
<tr>
<td>Firewall Throughput</td>
<td>10 Gbps</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>Concurrent Sessions</td>
<td>5,000</td>
<td>5,000</td>
</tr>
<tr>
<td>IPsec Policies</td>
<td>1,000</td>
<td>1,000</td>
</tr>
<tr>
<td>Gateway-to-Gateway IPsec VPN Tunnels</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>Client-to-Gateway IPsec VPN Tunnels</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>Concurrent SSL-VPN Users</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>SSL Inspection Throughput</td>
<td>700 Mcps</td>
<td>700 Mcps</td>
</tr>
<tr>
<td>SSL Inspection CS</td>
<td>400</td>
<td>400</td>
</tr>
<tr>
<td>SSL Inspection Concurrent Session</td>
<td>700 Mcps</td>
<td>700 Mcps</td>
</tr>
<tr>
<td>Application Control Throughput (HTTP 64K)</td>
<td>1.8 Gbps</td>
<td>1.8 Gbps</td>
</tr>
<tr>
<td>CAPWAP Throughput (HTTP 64K)</td>
<td>8 Gbps</td>
<td>8 Gbps</td>
</tr>
<tr>
<td>Virtual Domains (Default / Maximum)</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Maximum Number of FortiSwitches Supported</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Maximum Number of FortiAPs (Total / Tunnel Mode)</td>
<td>64 / 32</td>
<td>64 / 32</td>
</tr>
<tr>
<td>Maximum Number of FortiTokens</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>High Availability Configurations</td>
<td>Active / Active / Active / Passive, Clustering</td>
<td>Active / Active / Active / Passive, Clustering</td>
</tr>
</tbody>
</table>

### 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 mm
- Weight: 2.23 lbs (1.01 kg)

### Radio Specifications

- Multiple User (MU) MIMO: 3x3
- Maximum Wi-Fi SSID: 1300 Mpps @ 5 GHz, 450 Mpps @ 2.4 GHz
- Maximum Tx Power: 20 dBm
- Antenna Gain: 3.5 dBi @ 5 GHz, 5 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>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 60F</td>
<td>FG-60F</td>
<td>10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum managed FortiAPs (Total / Tunnel) 30 / 10.</td>
</tr>
<tr>
<td>FortiGate 61F</td>
<td>FG-61F</td>
<td>10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum managed FortiAPs (Total / Tunnel) 30 / 10.</td>
</tr>
<tr>
<td>FortiWiFi 60F</td>
<td>FWF-60F</td>
<td>10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum managed FortiAPs (Total / Tunnel) 10 / 10.</td>
</tr>
<tr>
<td>FortiWiFi 61F</td>
<td>FWF-61F</td>
<td>10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum managed FortiAPs (Total / Tunnel) 10 / 10.</td>
</tr>
</tbody>
</table>

Optional Accessories

- **Rack Mount Tray**
  - SP-RACKTRAY-02
  - Rack mount tray for all FortiGate E series and F series desktop models and backward compatible with SP-RackTray-01. For list of compatible FortiGate products, visit our Documentation website, docs.fortinet.com

Order Information

**Bundles**

- **FortiGuard Bundle**
  - FortiCare
  - 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 Protection
  - FortiGuard IoT Detection Service
  - FortiConverter Service
  - IPAM Cloud
  - SD-WAN Orchestrator Entitlement
  - SD-WAN Cloud Assisted Monitoring
  - SD-WAN Overlay Controller VPN Service
  - FortiAnalyzer Cloud
  - FortiManager Cloud

**FortiGuard Labs**

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.