The FortiGate 80F 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
- 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

### 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

<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>900 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, and 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 identifies anomalies
- Strong security posture with next generation firewall and real-time threat protection
Hardware

FortiGate 80F/80F-Bypass/81F

**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. 2x GE RJ45/SFP Shared Media Ports
2. 1x Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)*
3. 6x GE RJ45 Ports
4. 2x GE RJ45 FortiLink Ports

*80F-Bypass model only

**Bypass WAN/LAN Mode**

The FortiGate-80F-Bypass offers a pair of bypass ports that help organizations avoid network communication interruption due to device faults and improve network reliability.

**3G/4G WAN Connectivity**

The FortiGate 80F Series includes a 3.0 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.
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 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 80F</th>
<th>FORTIGATE 80F-BYPASS</th>
<th>FORTIGATE 81F</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE RJ45/SFP Shared Media Pairs</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>GE RJ45 Internal Ports</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>GE RJ45 FortiLink Ports (Default)</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Bypass GE RJ45 Port Pair (WAN1 &amp; Port1, default configuration)</td>
<td>–</td>
<td>–</td>
<td>Tx 128 GB SSD</td>
</tr>
<tr>
<td>USB Ports 3.0</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>
</tr>
<tr>
<td>Internal Storage</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

## System Performance — Enterprise Traffic Mix

| IPS Throughput | 1.4 Gbps |
| IPS Performance Test | 1.4 Gbps |
| Threat Protection Throughput | 900 Mbps |

## System Performance

### Firewall Throughput (1518 / 512 / 64 byte UDP packets)

| Firewall Throughput | 10/10/7 Gbps |
| Firewall Throughput (Packets Per Second) | 10.5 Mbps |
| Concurrent Sessions (TCP) | 1.5 Million |
| New Sessions/Second (TCP) | 2,500 |
| Firewalls | 10 |
| IPSec VPN Throughput (512 byte) | 6.5 Gbps |
| Gateway-to-Gateway IPSec VPN Tunnels | 400 |
| Client-to-Gateway IPSec VPN Tunnels | 2,500 |
| SSL-VPN Throughput | 950 Mbps |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | 200 |
| SSL Inspection Throughput (IPS, avg. HTTPS) | 715 Mbps |
| SSL Inspection CPS (IPS, avg. HTTPS) | 700 |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) | 100,000 |
| Application Control Throughput (HTTP 64K) | 1.8 Gbps |
| CAPWAP Throughput (HTTP 64K) | 9 Gbps |
| Virtual Domains (Default / Maximum) | 10 / 10 |
| Maximum Number of FortiSwitches Supported | 16 |
| Maximum Number of FortiAPs (Total / Tunnel Mode) | 32 / 16 |
| Maximum Number of FortiTokens | 500 |

## 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 |
| Weight | 1.1 lbs (2.4 kg) |
| Form Factor | Desktop/Wall Mount/Rack Tray |

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, URL filtering, and Malware Protection with sandboxing enabled.
## Specifications

### Operating Environment and Certifications

<table>
<thead>
<tr>
<th></th>
<th>FORTIGATE 80F</th>
<th>FORTIGATE 80F-BYPASS</th>
<th>FORTIGATE 81F</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input Rating</strong></td>
<td>Dual power 12Vdc, 3A</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Power Required</strong></td>
<td>Powered by 2 External DC Power Adapters, 100–240V AC, 50/60 Hz</td>
<td>100–240V AC, 50/60 Hz</td>
<td>100–240V AC, 50/60 Hz</td>
</tr>
<tr>
<td><strong>Heat Dissipation</strong></td>
<td>54.4 BTU/h</td>
<td>49.9 BTU/h</td>
<td>57.6 BTU/h</td>
</tr>
<tr>
<td><strong>Operating Temperature</strong></td>
<td>32–104°F (-0–40°C)</td>
<td>32–104°F (-0–40°C)</td>
<td>32–104°F (-0–40°C)</td>
</tr>
<tr>
<td><strong>Storage Temperature</strong></td>
<td>-20–71°F (-28–22°C)</td>
<td>-20–71°F (-28–22°C)</td>
<td>-20–71°F (-28–22°C)</td>
</tr>
<tr>
<td><strong>Humidity</strong></td>
<td>10–90% non-condensing</td>
<td>10–90% non-condensing</td>
<td>10–90% non-condensing</td>
</tr>
<tr>
<td><strong>Noise Level</strong></td>
<td>42 dB</td>
<td>42 dB</td>
<td>42 dB</td>
</tr>
<tr>
<td><strong>Operating Altitude</strong></td>
<td>Up to 3,000 ft (914 m)</td>
<td>Up to 3,000 ft (914 m)</td>
<td>Up to 3,000 ft (914 m)</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>FCC, ICES, CE, RCM, VCCI, BSMI, OU/RK, CB</td>
<td>FCC, ICES, CE, RCM, VCCI, BSMI, OU/RK, CB</td>
<td>FCC, ICES, CE, RCM, VCCI, BSMI, OU/RK, CB</td>
</tr>
<tr>
<td><strong>Certifications</strong></td>
<td>ECA Labs: Firewall, IATC, IPS, Antivirus, SSL-VPN</td>
<td>ECA Labs: Firewall, IATC, IPS, Antivirus, SSL-VPN</td>
<td>ECA Labs: Firewall, IATC, IPS, Antivirus, SSL-VPN</td>
</tr>
</tbody>
</table>

### Order Information

#### Product

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 80F</td>
<td>FG-80F</td>
<td>8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports</td>
</tr>
<tr>
<td>FortiGate 81F</td>
<td>FG-81F</td>
<td>8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports</td>
</tr>
<tr>
<td>FortiGate 80F-Bypass</td>
<td>FG-80F-Bypass</td>
<td>8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, may be configured with 1 pair of LAN bypass</td>
</tr>
</tbody>
</table>

#### Accessories

<table>
<thead>
<tr>
<th>Accessory</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC power adapter</td>
<td>SP-FG60E-PDC-5</td>
<td>Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61E, 80E/81E and 80F/81F</td>
</tr>
<tr>
<td>Rack Mount Tray</td>
<td>SP-RACKTRAY-02</td>
<td>Rack mount tray for all FortiGate E series and F series desktop models</td>
</tr>
<tr>
<td>Wall Mount Kit</td>
<td>SP-FG80F-MOUNT-20</td>
<td>Pack of 20 wall mount kits for FG/FWF-40F series, FG/FWF-60F series, FG-80F, FG-81F and FG-80F-Bypass</td>
</tr>
</tbody>
</table>

#### Transceivers

<table>
<thead>
<tr>
<th>Transceiver Module</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 GE SFP RJ45 Transceiver Module</td>
<td>RN-TRAN-GC</td>
<td>1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots</td>
</tr>
<tr>
<td>1 GE SFP LX Transceiver Module</td>
<td>RN-TRAN-LX</td>
<td>1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Bundles</th>
<th>360 Protection</th>
<th>Enterprise Protection</th>
<th>Unified Threat Protection</th>
<th>Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</td>
<td>AFE2</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
<tr>
<td>FortiGuard App Control Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Advanced Malware Protection (AMP) – Antivirus, Mobile Malware, Botnet, CDR, Viruses/General Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Industrial Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IoT Detection Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Orchestrator Entitlement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiAnalyzer Cloud Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiManager Cloud Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(1) 24/7 plus Advanced Services Ticket Handling (2) Available when running FortiOS 6.4