The FortiGate/FortiWiFi 40F 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
- 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

**Networks**
- 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

<table>
<thead>
<tr>
<th>Firewall</th>
<th>IPS</th>
<th>NGFW</th>
<th>Threat Protection</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Gbps</td>
<td>1 Gbps</td>
<td>800 Mbps</td>
<td>600 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 FortiManger 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

**Diagram:**
- Small Office Deployment (NGFW)
- Enterprise Branch Deployment (Secure SD-WAN)
HARDWARE

FortiGate FortiWiFi 40F-3G4G

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

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 the 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

3G/4G WAN Extensions

The FortiGate/FortiWiFi 40F-3G4G Series includes built-in 3G4G/LTE modem that allows 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 a superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Secure Access Layer

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 to regular ports as needed.
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 1000 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

**FORTIGATE 40F-3G4G**

<table>
<thead>
<tr>
<th>Interfaces and Modules</th>
<th>FORTIWIFI 40F-3G4G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Accelerated GE RJ45</td>
<td>1</td>
</tr>
<tr>
<td>WAN Ports</td>
<td>1</td>
</tr>
<tr>
<td>Hardware Accelerated GE RJ45</td>
<td>1</td>
</tr>
<tr>
<td>Internal Ports</td>
<td>3</td>
</tr>
<tr>
<td>Hardware Accelerated GE RJ45</td>
<td>1</td>
</tr>
<tr>
<td>FortiLink Ports</td>
<td>1</td>
</tr>
</tbody>
</table>

**Cellular Modem**

- 3G4G / LTE

**Wireless Interface**

- Single Radio
  - (2.4 GHz/5GHz), 802.11
  - a/b/g/h/ac-W2

**Antenna Ports (SMA)**

- 3

**USB Ports**

- 1

**Console Port (RJ45)**

- 1

**SIM Slots (Nano SIM)**

- 2

**Internal Storage**

- --

**System Performance — Enterprise Traffic Mix**

- **IPS Throughput**
  - 1 Gbps
- **NGFW Throughput**
  - 200 Mbps
- **Threat Protection Throughput**
  - 600 Mbps

**System Performance and Capacity**

- **IPv4 Firewall Throughput**
  - (1518 / 512 / 64 byte, UDP)
  - 5 / 5 / 5 Gbps
- **Firewall Latency**
  - (64 byte, UDP)
  - 2.97 μs
- **Firewall Throughput (Packet per Second)**
  - 75 Mpps
- **Concurrent Sessions**
  - 35000
- **Firewall Policies**
  - 5000
- **IPsec VPN Throughput (512 byte)**
  - 4.4 Gbps
- **Gateway-to-Gateway IPsec VPN Tunnels**
  - 200
- **Client-to-Gateway IPsec VPN Tunnels**
  - 250
- **SSL-VPN Throughput**
  - 490 Mbps
- **Concurrent SSL-VPN Users**
  - (Recommended Maximum, Tunnel Mode)
  - 200
- **SSL Inspection Throughput**
  - (IPS, avg. HTTPS)
  - 320 Mbps
- **SSL Inspection Concurrent Session**
  - (IPS, avg. HTTPS)
  - 55 000
- **Application Control Throughput**
  - (HTTP 64K)
  - 990 Mbps
- **CAPWAP Throughput (HTTP 64K)**
  - 3.5 Gbps
- **Virtual Domains (Default / Maximum)**
  - 10 / 10
- **Maximum Number of FortiSwitches Supported**
  - --
- **Maximum Number of FortiAPs**
  - (Total / Tunnel)
  - 16 / 8
- **Maximum Number of FortiTokens**
  - 500
- **High Availability Configurations**
  - Active-Active, Active-Passive, Clustering

**Dimensions and Power**

- **Height x Width x Depth (inches)**
  - 1.6 x 8.5 x 6.3
- **Weight**
  - 2.2 lbs (1 kg)
- **Form Factor**
  - Desktop
- **Cellular Modem**
  - 3G4G / LTE
- **Power Required**
  - Powered by external DC power adapter
  - 100-240V AC, 50/60 Hz
  - 100V AC / 0.3A, 240V AC / 0.2A
- **Power Consumption**
  - (Average / Maximum)
  - 15.8 W / 18.6 W
  - 18.6 W / 19.8 W
- **Heat Dissipation**
  - 63.5 BTU/h
  - 67.6 BTU/h

**System Compatibility**

- **Modules**
  - 100V AC / 0.3A, 240V AC / 0.2A
  - 100V AC / 0.3A, 240V AC / 0.2A
- **Antenna Gain**
  - Yes
- **GNSS Bias**
  - Yes

**Regional Compatibility**

- **Network Compatibility**
  - All Regions
  - Sierra Wireless EM7565
  - 2 SIM Slots, Active/Passive
- **LTE Category**
  - CAT-12
  - B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B18, B19, B20, B26, B28, B29, B30, B32, B41, B42, B43, B48
  - B66
  - B7, B8, B9, B19
- **CDMA**
  - 1xRTT/EV-DO Rev A
- **GSM/GPRS/EDGE**
  - 3G
- **WCDMA**
  - --

**Compatibility**

- **ICSA Labs**
  - Firewall, IPsec, IPS, Antivirus, SSL-VPN

**Radio Specifications**

- **Multiple (MU) MIMO**
  - 3x3
- **Maximum Wi-Fi Speeds**
  - 1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz
- **Maximum Tx Power**
  - 3.5 dB @ 5 GHz, 5 dB @ 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.
**ORDERING INFORMATION**

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 40F-3G4G</td>
<td>FG-40F-3G4G</td>
<td>5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports) with Embedded 3G/4G/LTE wireless wan module, external SMA WWAN antennas included</td>
</tr>
<tr>
<td>FortiWiFi 40F-3G4G</td>
<td>FWF-40F-3G4G-[RC]</td>
<td>5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports) with Embedded 3G/4G/LTE wireless wan module, Wireless (802.11a/b/g/n/ac-W2), external SMA WWAN and wireless antennas included</td>
</tr>
</tbody>
</table>

**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>Enterprise Protection</th>
<th>SMB Protection</th>
<th>Unified Threat Protection</th>
<th>Advanced Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGuard Enterprise Protection</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
<tr>
<td>FortiGuard SMB Protection</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
<tr>
<td>FortiGuard Unified Threat Protection</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
<tr>
<td>FortiGuard Advanced Threat Protection</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
</tbody>
</table>

1. Available when running FortiOS 7.0