The FortiGate 100F series combines next generation firewall and SD-WAN capabilities for mid-sized to large enterprise distributed locations. Powered by purpose-built Secure SD-WAN ASIC, FortiGate 100F delivers optimal performance for business-critical applications along with best security effectiveness.

**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 best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs, ICSA, Virus Bulletin and AV Comparatives

**Networking**
- Best of Breed SD-WAN capabilities to enable application steering using WAN path control for high quality of experience
- Delivers advanced networking capabilities, high-performance, and scalable IPsec VPN capabilities to consolidate networking and security

**Management**
- Includes management console that’s effective, simple to use, and provides comprehensive network automation & visibility.
- Provides Zero Touch Integration with 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
- 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>20 Gbps</td>
<td>2.6 Gbps</td>
<td>1.6 Gbps</td>
<td>1 Gbps</td>
<td>Multiple GE RJ45, GE SFP and 10 GE SFP+ slots</td>
</tr>
</tbody>
</table>

Refer to specification table for details
Deployment

Next Generation Firewall (NGFW)

- Reduce complexity by combining threat protection security capabilities into single high-performance network security appliance
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual applications in your network traffic
- Delivers industry's highest SSL inspection performance using industry-mandated ciphers while maximizing ROI
- Proactively blocks newly discovered sophisticated attacks in real-time with advanced threat protection

Secure SD-WAN

- Secure direct Internet access for Cloud applications for improved latency and reduce WAN cost spending
- High-performance and cost-effective threat protection capabilities
- WAN Path Controller and Link Health Monitoring for better application performance
- Security Processor powered industry's best IPsec VPN and SSL Inspection performance
- Simplified Management and Zero-Touch deployment

FortiGate 100F/101F deployment in Campus (NGFW)

FortiGate 100F/101F deployment in Enterprise Branch (Secure SD-WAN)
Hardware

FortiGate 100F/101F

**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

**Dual Power Supplies**
Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 100F Series offers dual built-in non-hot swappable power supplies.

**Interfaces**
1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/DMZ Ports
4. 2x GE RJ45 WAN Ports
5. 2x GE RJ45 HA Ports
6. 12x GE RJ45 Ports
7. 2x 10 GE SFP+ FortiLink Slots
8. 4x GE SFP Slots
9. 4x GE RJ45/SFP Shared Media Pairs
Fortinet Security Fabric

Security Fabric
The Security Fabric delivers broad visibility, integrated AI-driven breach prevention, and automated operations, orchestration, and response across all Fortinet and its ecosystem deployments. It allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between IoT, devices, and cloud environments throughout the network. All this is tied together under a single pane of glass management for significantly thereby delivering leading security capabilities across your entire environment while also significantly reducing complexity.

FortiGates are the foundation of Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet security products and Fabric-Ready Partner solutions.

FortiOS
Control all security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce complexity, costs, and response time with a truly consolidated next-generation security platform.

- A truly consolidated platform with a single OS and pane-of-glass for all security and networking services across all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance. Ability to leverage 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.
- Prevent, detect, and mitigate advanced attacks automatically in minutes with integrated AI-driven breach prevention and advanced threat protection.
- Improved user experience with innovative SD-WAN capabilities and ability to detect, contain and isolate threats with Intent-based Segmentation.
- Utilize SPU hardware acceleration to boost security capability performance.

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™ 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

### Hardware Specifications

<table>
<thead>
<tr>
<th>FORTIGATE 100F</th>
<th>FORTIGATE 101F</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE RJ45 Ports</td>
<td>12</td>
</tr>
<tr>
<td>GE RJ45 Management/DMZ Ports</td>
<td>1 / 2</td>
</tr>
<tr>
<td>GE SFP Slots</td>
<td>4</td>
</tr>
<tr>
<td>10GE SFP+ Slots</td>
<td>2</td>
</tr>
<tr>
<td>GE RJ45 WAN Ports</td>
<td>1 / 2 / 1</td>
</tr>
<tr>
<td>GE RJ45 or SFP Shared Ports</td>
<td>4</td>
</tr>
<tr>
<td>USB Port</td>
<td>0</td>
</tr>
<tr>
<td>Console Port</td>
<td>1</td>
</tr>
<tr>
<td>Internal Storage</td>
<td>1x 480 GB SSD</td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>0</td>
</tr>
</tbody>
</table>

### System Performance — Enterprise Traffic Mix

<table>
<thead>
<tr>
<th></th>
<th>FORTIGATE 100F</th>
<th>FORTIGATE 101F</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Throughput</td>
<td>2.6 Gbps</td>
<td></td>
</tr>
<tr>
<td>NGFW Throughput</td>
<td>1.8 Gbps</td>
<td></td>
</tr>
<tr>
<td>Threat Protection Throughput</td>
<td>1.6 Gbps</td>
<td></td>
</tr>
</tbody>
</table>

### System Performance

- **Firewall Throughput**: 20 / 18 / 10 Gbps
- **Firewall Latency**: 5 μs
- **Firewall Throughput (Packets Per Second)**: 1.5 Mpps
- **Firewall Policies**: 10,000
- **IPS Throughput**: 11.5 Gbps
- **Gateway-to-Gateway IPS/VPN Tunnels**: 2,500
- **Client-to-Gateway IPS/VPN Tunnels**: 70,000
- **SSL-VPN Throughput**: 150 Mbps
- **Concurrent SSL-VPN Users**: 300
- **SSL Inspection Throughput (IPS, avg. HTTPS)**: 1.3 Gbps
- **SSL Inspection CPS (IPS, avg. HTTPS)**: 1,800
- **SSL Inspection Concurrent Session (IPS, avg. HTTPS)**: 130,000
- **Application Control Throughput**: 1.0 Gbps
- **CAPNAP Throughput**: 15 Gbps
- **Virtual Domains (Default / Maximum)**: 10 / 10
- **Maximum Number of FortiSwitches Supported**: 64 / 32
- **Maximum Number of FortiTokens**: 5,000
- **Maximum Number of Registered FortiClients**: 500
- **Maximum Number of FortiClient Devices**: 1,000

### Dimensions

<table>
<thead>
<tr>
<th></th>
<th>FORTIGATE 100F</th>
<th>FORTIGATE 101F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height x Width x Length (inches)</td>
<td>1.73 x 17 x 10</td>
<td>1.83 x 17 x 10</td>
</tr>
<tr>
<td>Weight</td>
<td>7.25 lbs (3.29 kg)</td>
<td>7.36 lbs (3.43 kg)</td>
</tr>
</tbody>
</table>

### Environment

- **Power Required**: 100–240V AC, 60–50 Hz
- **Maximum Current**: 100V / 1A, 240V / 0.5A
- **Power Consumption (Average / Maximum)**: 35.1 W / 39.1 W
- **Heat Dissipation**: 119.77 BTU/h

- **Compliance**: FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSM
- **Certifications**: ICSA Labs: Firewall, IPS, Antivirus, SSL-VPN, IPv6

### High Availability Configurations

- Active / Active, Active / Passive, Clustering

---

* Copper SFP module is not supported.

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.
## Order Information

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 100F</td>
<td>FG-100F</td>
<td>22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media, 4 SFP ports, 2x 10 GE SFP+, FortiLinks, dual power supplies redundancy. Max managed FortiAPs (Total / Tunnel) 64 / 32.</td>
</tr>
<tr>
<td>FortiGate 101F</td>
<td>FG-101F</td>
<td>22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media, 4 SFP ports, 2x 10 GE SFP+, FortiLinks, 480 GB onboard storage, dual power supplies redundancy. Max managed FortiAPs (Total / Tunnel) 64 / 32.</td>
</tr>
</tbody>
</table>

### Optional Accessories

<table>
<thead>
<tr>
<th>Module Type</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 GE SFP LX transceiver module</td>
<td>FG-TRAN-LX</td>
<td>1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>1 GE SFP RJ45 transceiver module</td>
<td>FG-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 SX transceiver module</td>
<td>FG-TRAN-SX</td>
<td>1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>10 GE SFP+ transceiver module, short range</td>
<td>FG-TRAN-SFP+SR</td>
<td>10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.</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.

### 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></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard App Control Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IPS Service</td>
<td></td>
<td></td>
<td></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></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Web Filtering Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Antispam Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Security Rating 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>FortiCASB SaaS-only Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiConverter Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Cloud Assisted Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Overlay Controller VPN Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiAnalyzer Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiManager Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

---

Copyright © 2019 Fortinet, Inc. All rights reserved. FortiGate®, FortiGate® 100F Series, 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 in the same ideal conditions as in Fortinet's internal lab tests. 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. 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.

FST-PROD-D35-GTHS2