The FortiGate 100F series provides an application-centric, scalable and secure SD-WAN solution with next generation firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or enterprise branch level. 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

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
- 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>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 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 Web Gateway (SWG)**
- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL’s and domains
- Prevent data loss and discover user activity to known and unknown cloud applications
- Block DNS requests against malicious domains
- Multi-layered advanced protection against zero-day malware threats delivered over the web

**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 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.

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.

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 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 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

**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 M-ports (DMZ Ports)</td>
<td>1/2/1</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>2</td>
</tr>
<tr>
<td>GE RJ45 or SFP Shared Ports</td>
<td>4</td>
</tr>
<tr>
<td>USB Port</td>
<td>1</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**

- **IPS Throughput**: 2.6 Gbps
- **NGFW Throughput**: 1.8 Gbps
- **Threat Protection Throughput**: 1.6 Gbps

**System Performance**

- **Firewall Throughput**: 20 / 18 / 10 Gbps
- **Firewall Throughput (Packet Per Second)**: 5,000
- **Concurrent Sessions (TCP)**: 24,000
- **New Sessions/Second (TCP)**: 56,000
- **Firewall Policies**: 10,000
- **IPSec VPN Throughput (512 bytes)**: 15 Mbps
- **Gateway-to-Gateway IPSec VPN Tunnels**: 250
- **Client-to-Gateway IPSec VPN Tunnels**: 250
- **SSL-VPN Throughput**: 0 Gbps
- **Concurrent SSL-VPN Users**: 500
  (Recommended: Maximum, Tunnel Mode)
- **SSL Inspection Throughput (IPS, avg. HTTPS)**: 1 Gbps
- **SSL Inspection Concurrent Session (IPS, avg. HTTPS)**: 10,000
- **Application Control Throughput (HTTP 64K)**: 15 Gbps
- **CAPNAP Throughput**: 10 Gbps
- **Virtual Domains (Default / Maximum)**: 10 / 10
- **Maximum Number of FortiSwitches Supported**: 24
- **Maximum Number of FortiAPs (Total / Tunnel Mode)**: 128 / 64
- **Maximum Number of FortiTokens**: 5,000
- **High Availability Configurations**: Active / Active, Active / Passive, Clustering

**Environment**

- **Dimensions**: 1.73 x 17 x 10
- **Temperature**: 32–104°F (0–40°C)
- **Humidity**: 10–90% non-condensing
- **Noise Level**: 40.4 dBA

**Compliance**

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

**Certifications**

- **Power Required**: 100–240V AC, 50-60 Hz
- **Maximum Current**: 100V / 1A, 240V / 0.5A
- **Power Consumption (Average / Maximum)**: 35.1 W / 39.1 W
- **Heat Dissipation**: 119.77 BTU/h
- **Redundant Power Supplies**: Yes
- **Environment**
  - **Operating Temperature**: 32–104°F (0–40°C)
  - **Storage Temperature**: -31–158°F (-35–70°C)
  - **Operating Altitude**: Up to 7,400 ft (2,250 m)
  - **Humidity**: 10–90% non-condensing
  - **Noise Level**: 40.4 dBA
- **Compliance**
  - **FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI**

* Copper SFP module is not supported.

Note: All performance values are “up to” and vary depending on system configuration.

1. IPS/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</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, 480GB onboard storage, dual power supplies redundancy</td>
</tr>
</tbody>
</table>

Optional Accessories

| 1 GE SFP LX transceiver module | FG-TRAN-LX | 1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots |
| 1 GE SFP RJ45 transceiver module | FG-TRAN-GC | 1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots |
| 1 GE SFP SX transceiver module | FG-TRAN-SX | 1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots |
| 10 GE SFP+ transceiver module, short range | FG-TRAN-SFP+SR | 10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots |

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>Unified Threat Protection</th>
<th>Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</td>
<td>24x7</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 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 Antivirus 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>FortiGuard IoT Detection 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>IPAM Cloud</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>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 when running FortiOS 6.4