The FortiGate 100E series delivers next generation firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or enterprise branch level. Protects against cyber threats with high-powered security processors for optimized network performance, security efficacy and deep visibility. 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

Next Generation Firewall
Secure SD-WAN
Secure Web Gateway

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

<table>
<thead>
<tr>
<th>Firewall</th>
<th>IPS</th>
<th>NGFW</th>
<th>Threat Protection</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.4 Gbps</td>
<td>500 Mbps</td>
<td>360 Mbps</td>
<td>250 Mbps</td>
<td>Multiple GE RJ45, 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 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

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
Hardware

**FortiGate 100E/101E**

- Custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today’s wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck

**Network Processor**

Fortinet’s new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:
- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency down to 2 microseconds
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

**Content Processor**

Fortinet’s new, breakthrough SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection of computationally intensive security features:
- Enhanced IPS performance with unique capability of full signature matching at ASIC
- SSL Inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading

**FortiGate 100EF**

**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. 8x GE RJ45 Ports
7. 8x GE SFP Slots

**FortiGate 100E-POE**

**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. 14x GE RJ45 Ports
7. 2x GE RJ45/SFP Shared Media Pairs

**Powered by SPU**

- Custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today’s wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck
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></th>
<th>FORTIGATE 100E</th>
<th>FORTIGATE 101E</th>
<th>FORTIGATE 100EF</th>
<th>FORTIGATE 140E-POE</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE RJ45 Ports</td>
<td>14</td>
<td>14</td>
<td>8</td>
<td>14</td>
</tr>
<tr>
<td>GE RJ45 Management/HA/DMZ Ports</td>
<td>2 / 2 / 1</td>
<td>2 / 2 / 1</td>
<td>2 / 2 / 1</td>
<td>2 / 1</td>
</tr>
<tr>
<td>GE RJ45 PoE+ Ports</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>GE RJ45 SFP Slots</td>
<td>—</td>
<td>—</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>GE RJ45 WAN Ports</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>USB Port</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Console Port</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Internal Storage</td>
<td>1x 480 GB SSD</td>
<td>—</td>
<td>1x 480 GB SSD</td>
<td>—</td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### System Performance — Enterprise Traffic Mix

<table>
<thead>
<tr>
<th></th>
<th>FORTIGATE 100E</th>
<th>FORTIGATE 101E</th>
<th>FORTIGATE 100EF</th>
<th>FORTIGATE 140E-POE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Throughput</td>
<td>2,000</td>
<td>500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NGFW Throughput</td>
<td>2,000</td>
<td>360</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Protection Throughput</td>
<td>2,000</td>
<td>250</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### System Performance

<table>
<thead>
<tr>
<th></th>
<th>FORTIGATE 100E</th>
<th>FORTIGATE 101E</th>
<th>FORTIGATE 100EF</th>
<th>FORTIGATE 140E-POE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput (1151 / 512 / 64 byte UDP packets)</td>
<td>7.4 / 7.4 / 4.4 Gbps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall Throughput (Packets Per Second)</td>
<td>8.6 Mbps</td>
<td>3.2 Mbps</td>
<td>2 Mbps</td>
<td></td>
</tr>
<tr>
<td>Concurrent Sessions (TCP)</td>
<td></td>
<td>12,000</td>
<td>10,000</td>
<td></td>
</tr>
<tr>
<td>New Sessions/Second (TCP)</td>
<td></td>
<td>42,000</td>
<td>39,000</td>
<td></td>
</tr>
<tr>
<td>Firewall Policies</td>
<td></td>
<td>500,000</td>
<td>450,000</td>
<td></td>
</tr>
<tr>
<td>IPSec VPN Throughput (512 byte)</td>
<td>4 Gbps</td>
<td>4 Gbps</td>
<td>4 Gbps</td>
<td></td>
</tr>
<tr>
<td>Gateway-to-Gateway IPSec VPN Tunnels</td>
<td>2,000</td>
<td>2,000</td>
<td>2,000</td>
<td></td>
</tr>
<tr>
<td>Client-to-Gateway IPSec VPN Tunnels</td>
<td>10,000</td>
<td>10,000</td>
<td>10,000</td>
<td></td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td></td>
<td>250 Mbps</td>
<td>250 Mbps</td>
<td></td>
</tr>
<tr>
<td>Concurrent SSL-VPN Users</td>
<td></td>
<td>500</td>
<td>500</td>
<td></td>
</tr>
</tbody>
</table>

### Dimensions

<table>
<thead>
<tr>
<th></th>
<th>1.75 x 17 x 10</th>
<th>1.75 x 17 x 10</th>
<th>1.75 x 17 x 10</th>
<th>1.75 x 17 x 15.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height x Width x Length (mm)</td>
<td>Rack Mount, 1 RU</td>
<td>Rack Mount, 1 RU</td>
<td>Rack Mount, 1 RU</td>
<td>Rack Mount, 1 RU</td>
</tr>
<tr>
<td>Weight</td>
<td>7.28 lbs (3.3 kg)</td>
<td>7.28 lbs (3.3 kg)</td>
<td>7.28 lbs (3.3 kg)</td>
<td>12.4 lbs (5.6 kg)</td>
</tr>
</tbody>
</table>

### Environment

<table>
<thead>
<tr>
<th></th>
<th>100 – 240V AC, 50 – 60 Hz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Input</td>
<td>100V / 0.52A, 240V / 0.22A</td>
</tr>
<tr>
<td>Maximum Current</td>
<td>100V / 1.05A, 240V / 0.45A</td>
</tr>
<tr>
<td>Total Available PoE Power Budget*</td>
<td>100V / 0.52A, 240V / 0.22A</td>
</tr>
<tr>
<td>Power Consumption (Average / Maximum)</td>
<td>23.0 W / 26.0 W, 51.9 VA</td>
</tr>
<tr>
<td>Heat Dissipation</td>
<td>97.6 BTU/hr</td>
</tr>
</tbody>
</table>

* Maximum loading on each PoE+ port is 30 W (802.3at).

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>Environment</th>
<th>FORTIGATE 100E</th>
<th>FORTIGATE 101E</th>
<th>FORTIGATE 100EF</th>
<th>FORTIGATE 140E-POE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Temperature</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>
<td>32–104°F (0–40°C)</td>
</tr>
<tr>
<td>Humidity</td>
<td>Up to 80% non-condensing</td>
<td>80% non-condensing</td>
<td>80% non-condensing</td>
<td>80% non-condensing</td>
</tr>
<tr>
<td>Noise Level</td>
<td>50.4 dBA</td>
<td>40.4 dBA</td>
<td>40.4 dBA</td>
<td>40.4 dBA</td>
</tr>
<tr>
<td>Compliance</td>
<td>FCC, ICES, CE, RoHS, GS, UL/cUL, CEB</td>
<td>FCC, ICES, CE, RoHS, GS, UL/cUL, CEB</td>
<td>FCC, ICES, CE, RoHS, GS, UL/cUL, CEB</td>
<td>FCC, ICES, CE, RoHS, GS, UL/cUL, CEB</td>
</tr>
<tr>
<td>Certifications</td>
<td>KCC, BSMI, VCCI, BSM, GS, CE, RoHS</td>
<td>KCC, BSMI, VCCI, BSM, GS, CE, RoHS</td>
<td>KCC, BSMI, VCCI, BSM, GS, CE, RoHS</td>
<td>KCC, BSMI, VCCI, BSM, GS, CE, RoHS</td>
</tr>
</tbody>
</table>

Order Information

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 100E</td>
<td>FG-100E</td>
<td>20 x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 2x Mgmt port, 14x switch ports), 2x Shared Media pairs (including 2x GE RJ45 ports, 2x SFP slots). Maximum managed FortiAPs (Total / Tunnel) 64 / 32.</td>
</tr>
<tr>
<td>FortiGate 101E</td>
<td>FG-101E</td>
<td>20 x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 2x Mgmt port, 14x switch ports), 2x Shared Media pairs (including 2x GE RJ45 ports, 2x SFP slots). Maximum managed FortiAPs (Total / Tunnel) 64 / 32.</td>
</tr>
<tr>
<td>FortiGate 100EF</td>
<td>FG-100EF</td>
<td>14x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 2x Mgmt port, 8x Internal switch ports), 8x SFP ports. Maximum managed FortiAPs (Total / Tunnel) 64 / 32.</td>
</tr>
<tr>
<td>FortiGate 140E-POE</td>
<td>FG-140E-POE</td>
<td>40x GE RJ45 ports (including 2x WAN ports, 1x Mgmt port, 24x SFP GE RJ45/GE PoE+ ports, 14x switch ports), 2x GE SFP DMZ slots, Maximum managed FortiAPs (Total / Tunnel) 64 / 32.</td>
</tr>
</tbody>
</table>

Optional Accessories

- External redundant AC power supply: RPS-100

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 Service
  - FortiGuard IoT Detection Service
  - FortiConverter Service
  - IPAM Cloud
  - SD-WAN Orchestrator Entitlement
  - SD-WAN Cloud Assisted Monitoring
  - SD-WAN Overlay Controller VPN Service

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and 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 cited herein were obtained 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 to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet excludes 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. 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-PRD-DS-GTHS2