The FortiGate 100E series delivers next generation firewall capabilities for mid-sized to large enterprises, with the flexibility to be deployed at the campus or enterprise branch. Protect against cyber threats with security processor powered high performance, security efficacy and deep visibility.

**Security**
- Protects against known exploits, malware and malicious websites using continuous threat intelligence provided by FortiGuard Labs security services
- Identify thousands of applications including cloud applications for deep inspection into network traffic
- Detects unknown attacks using dynamic analysis and provides automated mitigation to stop targeted attacks

**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**
- Delivers an extensive routing, switching, wireless controller and high performance IPsec VPN capabilities to consolidate networking and security functionality
- Enables flexible deployment such as Next Generation Firewall and Secure SD-WAN

**Management**
- Single Pane of Glass with Network Operations Center (NOC) view provides 360° visibility to identify issues quickly and intuitively
- 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 collaboratively integrate and provide end-to-end security across the entire attack surface
- 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 specification table for details
DEPLOYMENT

**Next Generation Firewall (NGFW)**

- Combines threat prevention security capabilities into single high performance network security appliance
- Reduces complexity by creating campus topology view and providing granular visibility of devices, users and threat information
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual content of your network traffic
- Delivers industry’s highest SSL inspection performance using industry-mandated ciphers
- Proactively detect malicious unknown threats using integrated cloud-based sandbox service

**Secure SD-WAN**

- Secure direct Internet access for Cloud applications for improved latency and reduce WAN cost spending
- Effective, cost-efficient and high performance threat prevention capabilities
- WAN Path Controller and Link Health Monitoring for better application performance
- Security Processor powered industry’s best IPsec VPN and SSL Inspection performance
- Centralized Management and Zero-Touch deployment
HARDWARE

FortiGate 100E/101E

- 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. 2x GE RJ45/SFP Shared Media Pairs

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. 2x GE RJ45/SFP Slots

FortiGate 140E

- Interfaces
  1. USB Port
  2. Console Port
  3. 2x GE RJ45 MGMT/HA Ports
  4. 2x GE RJ45 WAN Ports
  5. 38x GE RJ45 Ports
  6. 2x GE SFP DMZ Slots
  7. 8x GE SFP Slots

FortiGate 140E-POE

- Interfaces
  1. USB Port
  2. Console Port
  3. 2x GE RJ45 MGMT/HA Ports
  4. 2x GE RJ45 WAN Ports
  5. 14x GE RJ45 Ports
  6. 24x GE RJ45 POE Ports
  7. 2x GE SFP DMZ Slots

**Powered by SPU SoC3**

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Simplifies appliance design and enables breakthrough performance for smaller networks
- Supports firewall acceleration across all packet sizes for maximum throughput
- Delivers accelerated UTM content processing for superior performance and protection
- Accelerates VPN performance for high speed, secure remote access

**Redundant Power Supply**

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 100E Series offers the option to connect to an external redundant power supply appliance — The FortiRPS 100, designed to increase network availability and uptime.
FORTINET SECURITY FABRIC

Security Fabric
The Security Fabric 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.

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 the security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce operating expenses and save time with a truly consolidated next-generation security platform.

- A truly consolidated platform with one OS for all security and networking services for all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings.
- Prevent, detect, and mitigate advanced attacks automatically in minutes with integrated advanced threat protection.
- Fulfill your networking needs with extensive routing, switching, and SD-WAN capabilities.
- Utilize SPU hardware acceleration to boost security capability performance.

For more information, please refer to the FortiOS data sheet available at www.fortinet.com

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.

For more information, please refer to fortinet.com

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/forticare
### SPECIFICATIONS

<table>
<thead>
<tr>
<th>Hardware Specifications</th>
<th>FORTIGATE 100E</th>
<th>FORTIGATE 101E</th>
<th>FORTIGATE 100EF</th>
<th>FORTIGATE 140E</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>38</td>
<td>14</td>
</tr>
<tr>
<td>GE RJ45 Management/HA/DMZ Ports</td>
<td>1 / 2 / 1</td>
<td>1 / 2 / 1</td>
<td>1 / 1 / —</td>
<td>1 / 1 / —</td>
<td>1 / 1 / —</td>
</tr>
<tr>
<td>GE SFP Slots</td>
<td>—</td>
<td>—</td>
<td>8</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>GE RJ45 Wan Ports</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>GE RJ45 or SFP Shared Ports</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>USB Port</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Console Port</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Internal Storage</td>
<td>—</td>
<td>—</td>
<td>1x 480 GB SSD</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System Performance — Enterprise Traffic Mix</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPS Throughput¹</td>
<td>500 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NGFW Throughput², ⁴</td>
<td>360 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Protection Throughput², ⁵</td>
<td>250 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall Throughput (1518 / 512 / 64 byte UDP packets)</td>
<td>7.4 / 7.4 / 4.4 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall Latency (64 byte UDP packets)</td>
<td>3 μs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall Throughput (Packets Per Second)</td>
<td>6.6 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concurrent Sessions (TCP)</td>
<td>135</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Sessions/Second (TCP)</td>
<td>300</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall Policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPSec VPN Throughput (512 byte)</td>
<td>10 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway-to-Gateway IPSec VPN Tunnels</td>
<td>2,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client-to-Gateway IPSec VPN Tunnels</td>
<td>10,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td>250 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concurrent SSL-VPN Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL Inspection Throughput (IPS, avg. HTTPS)</td>
<td>130 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL Inspection Concurrent Session (IPS, avg. HTTPS)</td>
<td>125,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Control Throughput (HTTP 844)</td>
<td>1 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAPWAP Throughput (1444 byte, UDP)</td>
<td>1.5 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Domains (Default / Maximum)</td>
<td>10 / 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Number of Switches Supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Number of FortiAPs (Total / Tunnel Mode)</td>
<td>64 / 32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Number of FortiTokens</td>
<td>1,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Number of Registered FortiClients</td>
<td>600</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High Availability Configurations</td>
<td>Active / Active, Active / Passive, Clustering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Height x Width x Length (inches)</td>
<td>1.75 x 17 x 10</td>
<td>1.75 x 17 x 10</td>
<td>1.75 x 17 x 10</td>
<td>1.75 x 17 x 15.5</td>
<td>1.75 x 17 x 15.5</td>
</tr>
<tr>
<td>Rack Mount, 1 RU</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>
<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>
<td>12.4 lbs (5.6 kg)</td>
</tr>
</tbody>
</table>

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</th>
<th>FORTIGATE 140E-POE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Required</td>
<td>100–240V AC, 60–50 Hz</td>
<td>100–240V AC, 50–60 Hz</td>
<td>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>Maximum Current</td>
<td>1 A (24 V DC)</td>
<td>1 A (24 V DC)</td>
<td>1 A (24 V DC)</td>
<td>1 A (24 V DC)</td>
<td>1 A (24 V DC)</td>
</tr>
<tr>
<td>Total Available PoE Power Budget*</td>
<td>30 W</td>
<td>30 W</td>
<td>30 W</td>
<td>30 W</td>
<td>30 W</td>
</tr>
<tr>
<td>Power Consumption (Average / Maximum)</td>
<td>7.0 W / 11.0 W</td>
<td>7.0 W / 11.0 W</td>
<td>7.0 W / 11.0 W</td>
<td>11.8 W / 26.0 W</td>
<td>17.06 W / 35.0 W</td>
</tr>
<tr>
<td>Heat Dissipation</td>
<td>35°–40°F (1°–4°C)</td>
<td>35°–40°F (1°–4°C)</td>
<td>35°–40°F (1°–4°C)</td>
<td>35°–40°F (1°–4°C)</td>
<td>35°–40°F (1°–4°C)</td>
</tr>
<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>
<td>32–104°F (0–40°C)</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-31–158°F (-35–70°C)</td>
<td>-31–158°F (-35–70°C)</td>
<td>-31–158°F (-35–70°C)</td>
<td>-31–158°F (-35–70°C)</td>
<td>-31–158°F (-35–70°C)</td>
</tr>
<tr>
<td>Noise Level</td>
<td>40.4 dBA</td>
<td>40.4 dBA</td>
<td>40.4 dBA</td>
<td>40.4 dBA</td>
<td>57 dBA</td>
</tr>
<tr>
<td>Humidity</td>
<td>10–90% non-condensing</td>
<td>10–90% non-condensing</td>
<td>10–90% non-condensing</td>
<td>10–90% non-condensing</td>
<td>10–90% non-condensing</td>
</tr>
<tr>
<td>Operating Altitude</td>
<td>Up to 14,000 ft (2,520 m)</td>
<td>Up to 14,000 ft (2,520 m)</td>
<td>Up to 14,000 ft (2,520 m)</td>
<td>Up to 14,000 ft (2,520 m)</td>
<td>Up to 14,000 ft (2,520 m)</td>
</tr>
<tr>
<td>Certifications</td>
<td>ICSA Labs: Firewall, Pisc, IPS, Antivirus, SSL, VNP, PIV</td>
<td>ICSA Labs: Firewall, Pisc, IPS, Antivirus, SSL, VNP, PIV</td>
<td>ICSA Labs: Firewall, Pisc, IPS, Antivirus, SSL, VNP, PIV</td>
<td>ICSA Labs: Firewall, Pisc, IPS, Antivirus, SSL, VNP, PIV</td>
<td>ICSA Labs: Firewall, Pisc, IPS, Antivirus, SSL, VNP, PIV</td>
</tr>
</tbody>
</table>

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

## 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, 1x Mgmt port, 2x HA ports, 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 HA ports, 1x switch ports), 2x Shared Media pairs (including 2x GE RJ45 ports, 2x SFP slots). 480 GB onboard storage. 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 HA ports, 8x internal switch ports), 8x SFP ports. Maximum managed FortiAPs (Total / Tunnel): 64 / 32.</td>
</tr>
<tr>
<td>FortiGate 140E</td>
<td>FG-140E</td>
<td>42x GE RJ45 ports (including 2x WAN ports, 1x Mgmt port, 1x HA port, 38x switch ports), 2x GE SFP DMZ ports. Maximum managed FortiAPs (Total / Tunnel): 64 / 32.</td>
</tr>
<tr>
<td>FortiGate 140E-POE</td>
<td>FG-140E-POE</td>
<td>42x GE RJ45 ports (including 2x WAN ports, 1x Mgmt port, 1x HA port, 24x RJ45 GE Poe/Poe+ ports, 14x switch ports), 2x GE SFP DMZ ports. Maximum managed FortiAPs (Total / Tunnel): 64 / 32.</td>
</tr>
</tbody>
</table>

### Optional Accessories

- **External redundant AC power supply**

### Bundles

- **FortiGuard Security Rating Service**
- **FortiGuard Web Filtering**
- **FortiGuard Industrial Service**
- **FortiGuard Advanced Malware Protection (AMP)** — Antivirus, Mobile Malware, Botnet, CDR*, Virus Outbreak Protection* and FortiSandbox Cloud Service*
- **FortiCare + FortiGuard App Control Service**

### 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.

### Polygons

- **FortiCASB SaaS-only Service**
- **FortiGuard Industrial Service**
- **FortiGuard Web Filtering**
- **FortiGuard Security Rating Service**
- **FortiGuard Advanced Malware Protection (AMP)** — Antivirus, Mobile Malware, Botnet, CDR*, Virus Outbreak Protection* and FortiSandbox Cloud Service*
- **FortiCare + FortiGuard App Control Service**

**Bundles**

- **Threat Protection**
- **UTM**
- **Enterprise Protection**

### Contact Information

- **GLOBAL HEADQUARTERS**
  - Fortinet Inc.
  - 899 KIFER ROAD
  - Sunnyvale, CA 94086
  - United States
  - Tel: +1.408.235.7700
  - www.fortinet.com/sales

- **EMEA SALES OFFICE**
  - 905 rue Albert Einstein
  - 06650 Valbonne
  - France
  - Tel: +33.4.8987.0500
  - www.fortinet.com/emea

- **APAC SALES OFFICE**
  - 8 Temasek Boulevard
  - #12-01 Suntec Tower Three
  - Singapore 038988
  - Tel: +65.6395.2788
  - www.fortinet.com/apac

- **LATIN AMERICA SALES OFFICE**
  - Sawgrass Lakes Center
  - 13450 W. Sunrise Blvd., Suite 430
  - Sunrise, FL 33323
  - United States
  - Tel: +1.954.368.9990

### Copyright

© 2018 Fortinet, Inc. All rights reserved. FortiGate®, FortiGate™, FortiFiShell® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Forti names herein may also be registered and/or common law trademarks of Fortinet. All other products and 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 into a 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements hereunder are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant herein, 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-DS-GT1HS2

**FORTINET 100E Series**

* Available when running FortiOS 6.0.1 and above  * With new Q3-2018 SKUs

---

[FortiGate® 100E Series Specifications](#)