The FortiGate 80E series offers an excellent Security and SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. Protect against cyber threats with industry-leading secure SD-WAN in a simple, affordable and easy to deploy solution.

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

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

The FortiGate 80E series offers an excellent Security and SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. Protect against cyber threats with industry-leading secure SD-WAN in a simple, affordable and easy to deploy solution.

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

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>4 Gbps</td>
<td>450 Mbps</td>
<td>360 Mbps</td>
<td>250 Mbps</td>
<td>Multiple GE RJ45</td>
</tr>
</tbody>
</table>

Refer to specification table for details
Deployment

Unified Threat Management (UTM)

- Integrated wired and wireless networking to simplify IT
- Purpose-built hardware for industry best performance with easy administration through cloud management
- Provides consolidated security and networking for small businesses and consistently provides top-rated threat protection
- 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 and quality of experience
- Security Processor powered industry's best IPsec VPN and SSL Inspection performance
- Simplified Management and Zero Touch deployment
Hardware

FortiGate 80E/81E

1. Console Port
2. USB Port
3. 12x GE RJ45 Ports
4. 2x GE RJ45 DMZ/HA Ports
5. 2x GE RJ45/SFP Shared Media Pairs

FortiGate 80E/81E-POE

1. Console Port
2. USB Port
3. 12x GE RJ45 PoE/+ Ports
4. 2x GE RJ45 DMZ/HA Ports
5. 2x GE RJ45/SFP Shared Media Pairs

Interfaces

1. Console Port
2. USB Port
3. 12x GE RJ45 PoE/+ Ports
4. 2x GE RJ45 DMZ/HA Ports
5. 2x GE RJ45/SFP Shared Media Pairs

Powered by SPU SoC3

- Combines a RISC-based CPU with Fortinet's proprietary 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

3G/4G WAN Connectivity

The FortiGate 80E Series includes a USB port that allows you to plug in a compatible third-party 3G/4G USB modem, providing 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 superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.
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

<table>
<thead>
<tr>
<th>Hardware Specifications</th>
<th>FORTIGATE 80E</th>
<th>FORTIGATE 80E-POE</th>
<th>FORTIGATE 81E</th>
<th>FORTIGATE 81E-POE</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE RJ45/SFP Shared Media Pairs</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>GE RJ45 Ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GE RJ45 PoE+ Ports</td>
<td>12</td>
<td></td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>GE RJ45 DMZ/HA Ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USB Ports</td>
<td>12</td>
<td></td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Console (RJ45)</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Internal Storage</td>
<td>—</td>
<td></td>
<td>1x 128 GB SSD</td>
<td></td>
</tr>
<tr>
<td><strong>System Performance — Enterprise Traffic Mix</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPS Throughput</td>
<td></td>
<td></td>
<td>450 Mbps</td>
<td></td>
</tr>
<tr>
<td>NGFW Throughput</td>
<td>4</td>
<td></td>
<td>360 Mbps</td>
<td></td>
</tr>
<tr>
<td>Threat Protection Throughput</td>
<td>5</td>
<td></td>
<td>250 Mbps</td>
<td></td>
</tr>
<tr>
<td><strong>System Performance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall Throughput (1518 / 512 / 64 byte UDP packets)</td>
<td>4 / 4 / 4 Gbps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall Throughput (Packets Per Second)</td>
<td>6 Gbps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concurrent Sessions (TCP)</td>
<td>1.3 Million</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Sessions/Second (TCP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall Policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPsec VPN Throughput (512 byte)</td>
<td>2.5 Gbps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway-to-Gateway IPsec VPN Tunnels</td>
<td>2.5 Gbps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client-to-Gateway IPsec VPN Tunnels</td>
<td>2.5 Gbps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td>200</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)</td>
<td>200</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL Inspection Throughput (IPS, avg. HTTPS)</td>
<td>135 Mbps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL Inspection CPS (IPS, avg. HTTPS)</td>
<td>135</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL Inspection Concurrent Session (IPS, avg. HTTPS)</td>
<td>50,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Control Throughput (HTTP 64K)</td>
<td>300 Mbps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAPWAP Throughput (HTTP 64K)</td>
<td>300 Mbps</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>
</tr>
<tr>
<td>Maximum Number of FortiSwitches Supported</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Number of FortiAPs (Total / Tunnel Mode)</td>
<td>32 / 16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Number of FortiTokens</td>
<td>500</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Number of Registered FortiClients</td>
<td>200</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>High Availability Configurations</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active / Active / Active / Passive / Clustering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dimensions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Height x Width x Length (inches)</td>
<td>1.65 x 8.5 x 7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Height x Width x Length (mm)</td>
<td>42.0 x 216 x 178</td>
<td></td>
<td></td>
<td></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 80E</th>
<th>FORTIGATE 80E-POE</th>
<th>FORTIGATE 81E</th>
<th>FORTIGATE 81E-POE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Required</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>100V AC / 0.25A, 240V AC / 0.11A</td>
<td>115V AC / 0.3A, 230V AC / 0.13A</td>
<td>100V AC / 0.25A, 240V AC / 0.11A</td>
<td>115V AC / 0.3A, 230V AC / 0.13A</td>
</tr>
<tr>
<td>Total Available PoE Power Budget*</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Power Consumption (Average / Maximum)</td>
<td>18 W / 25 W</td>
<td>20 / 137 W</td>
<td>20 W / 72 W</td>
<td>20 / 137 W</td>
</tr>
<tr>
<td>Heat Dissipation</td>
<td>40.5 BTU/h</td>
<td>245 BTU/h</td>
<td>46.5 BTU/h</td>
<td>245 BTU/h</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>
</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>
</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>
</tr>
<tr>
<td>Noise Level</td>
<td>Fanless 0 dBA</td>
<td>35 dBA Fanless 0 dBA</td>
<td>35 dBA Fanless 0 dBA</td>
<td>35 dBA Fanless 0 dBA</td>
</tr>
<tr>
<td>Operating Altitude</td>
<td>Up to 16,404 ft (5,000 m)</td>
<td>Up to 16,404 ft (5,000 m)</td>
<td>Up to 16,404 ft (5,000 m)</td>
<td>Up to 16,404 ft (5,000 m)</td>
</tr>
</tbody>
</table>

Order Information

**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.

- **FortiCare**: 24x7 plus Advanced Services Ticket Handling
- **FortiGuard App Control Service**: Up to 16,404 ft (5,000 m)
- **FortiGuard IPS Service**: 16 GB onboard storage
- **FortiGuard Advanced Malware Protection (AMP)**: Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service
- **FortiGuard Web Filtering Service**: 16 GB onboard storage
- **FortiGuard Antispam Service**: Maximum managed FortiAPs (Total/Tunnel) 32/16
- **FortiGuard Security Rating Service**: FortiAnalyzer Cloud 2
- **FortiGuard Industrial Service**: FortiCASB Saas-only Service
- **FortiConverter Service**: SD-WAN Overlay Controller VPN Service 2
- **FortiAnalyzer Cloud 2**: SD-WAN Cloud Assisted Monitoring 2

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

**Product** | **SKU** | **Description** | **360 Protection** | **Enterprise Protection** | **UTM Protection** | **Threat Protection**
---|---|---|---|---|---|---
FortiGate 80E | FG-80E | 14x GE RJ45 ports (including 1x DMZ port, 1x Mgmt port, 1x HA port, 12x switch ports), 2x Shared Media pairs (including 2x GE RJ45 ports, 2x SFP slots), Maximum managed FortiAPs (Total/Tunnel) 32/16. | | | | |
FortiGate 80E-PoE | FG-80E-POE | 16 GB onboard storage, Maximum managed FortiAPs (Total/Tunnel) 32/16. | | | | |
FortiGate 81E | FG-81E | 16x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x HA port, 12x PoE ports). Maximum managed FortiAPs (Total/Tunnel) 32/16. | | | | |
FortiGate 81E-PoE | FG-81E-POE | 128 GB onboard storage, Maximum managed FortiAPs (Total/Tunnel) 32/16. | | | | |

Copyright © 2019 Fortinet, Inc. All rights reserved. FortiGate® and FortiCare®, FortiGuard® and FortiGate®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet marks 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 to performance in the same ideal conditions as in Fortinet’s internal lab tests. 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.