The FortiGate 80E series provides an application-centric, scalable and secure SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. 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

**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>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 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 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 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

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 and 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 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

<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>12</td>
<td>—</td>
<td>12</td>
<td>—</td>
</tr>
<tr>
<td>GE RJ45 PoE+/ Ports</td>
<td>—</td>
<td>12</td>
<td>—</td>
<td>12</td>
</tr>
<tr>
<td>GE RJ45 DMZ/HA Ports</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>USB Ports</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Console (RJ45)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Internal Storage</td>
<td>—</td>
<td>—</td>
<td>1x 128 GB SSD</td>
<td>1x 128 GB SSD</td>
</tr>
</tbody>
</table>

**System Performance — Enterprise Traffic Mix**

| IPS Throughput | 450 Mbps |
| NGFW Throughput | 360 Mbps |
| Threat Protection Throughput | 250 Mbps |

<table>
<thead>
<tr>
<th>System Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput (1518 / 512 / 64 byte UDP packets)</td>
</tr>
<tr>
<td>Firewall Throughput (Packets Per Second)</td>
</tr>
<tr>
<td>Concurrent Sessions (TCP)</td>
</tr>
<tr>
<td>New Sessions/Second (TCP)</td>
</tr>
<tr>
<td>IPSec VPN Throughput (512 byte)</td>
</tr>
<tr>
<td>Gateway-to-Gateway IPSec VPN Tunnels</td>
</tr>
<tr>
<td>Client-to-Gateway IPSec VPN Tunnels</td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
</tr>
<tr>
<td>Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)</td>
</tr>
<tr>
<td>SSL Inspection Throughput (IPS, avg. HTTPS)</td>
</tr>
<tr>
<td>SSL Inspection CPS (IPS, avg. HTTPS)</td>
</tr>
<tr>
<td>SSL Inspection Concurrent Session (IPS, avg. HTTPS)</td>
</tr>
<tr>
<td>Application Control Throughput (HTTP 64K)</td>
</tr>
<tr>
<td>CAPWAP Throughput (HTTP 64K)</td>
</tr>
<tr>
<td>Virtual Domains (Default / Maximum)</td>
</tr>
<tr>
<td>Maximum Number of FortiSwitches Supported</td>
</tr>
<tr>
<td>Maximum Number of FortiAPs (Total / Tunnel Mode)</td>
</tr>
<tr>
<td>Maximum Number of FortiTokens</td>
</tr>
</tbody>
</table>

**High Availability Configurations**

<table>
<thead>
<tr>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height x Width x Length (inches)</td>
</tr>
<tr>
<td>Height x Width x Length (mm)</td>
</tr>
<tr>
<td>Weight</td>
</tr>
<tr>
<td>Form Factor</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><strong>Input Rating</strong></td>
<td>12Vdc, 3A</td>
<td>54Vdc, 2.78A</td>
<td>12Vdc, 3A</td>
<td>54Vdc, 2.78A</td>
</tr>
<tr>
<td><strong>Power Consumption (Average / Maximum)</strong></td>
<td>20W / 137W</td>
<td>100W / 137W</td>
<td>115W / 137W</td>
<td>100W / 137W</td>
</tr>
<tr>
<td><strong>Heat Dissipation</strong></td>
<td>85.3 BTU/h</td>
<td>110 W</td>
<td>85.3 BTU/h</td>
<td>110 W</td>
</tr>
<tr>
<td><strong>Operating Altitude</strong></td>
<td>54Vdc, 2.78A</td>
<td>12Vdc, 3A</td>
<td>54Vdc, 2.78A</td>
<td>12Vdc, 3A</td>
</tr>
<tr>
<td><strong>Humidity</strong></td>
<td>92.1 BTU/h</td>
<td>115W / 137W</td>
<td>92.1 BTU/h</td>
<td>115W / 137W</td>
</tr>
<tr>
<td><strong>Storage Temperature</strong></td>
<td>110 W</td>
<td>100W / 137W</td>
<td>110 W</td>
<td>100W / 137W</td>
</tr>
<tr>
<td><strong>Noise Level</strong></td>
<td>54Vdc, 2.78A</td>
<td>12Vdc, 3A</td>
<td>54Vdc, 2.78A</td>
<td>12Vdc, 3A</td>
</tr>
<tr>
<td><strong>Certifications</strong></td>
<td>110 W</td>
<td>100W / 137W</td>
<td>110 W</td>
<td>100W / 137W</td>
</tr>
</tbody>
</table>

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

### Order Information

#### Product

- **FORTIGATE 80E**: FG-80E
- **FORTIGATE 80E-POE**: FG-80E-POE
- **FORTIGATE 81E**: FG-81E
- **FORTIGATE 81E-POE**: FG-81E-POE

#### Optional Accessories

- **1 GE SFP RJ45 Transceiver Module**: FN-TRAN-GC
- **1 GE SFP LX Transceiver Module**: FN-TRAN-LX
- **1 GE SFP SX Transceiver Module**: FN-TRAN-SX

#### Bundles

- **FortiGuard Bundles**
- **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**
- **FortiAnalyzer Cloud**
- **FortiManager Cloud**
- **SD-WAN Overlay Controller VPN Service**

#### Bundles Details

- **FortiGuard Cloud**
- **FortiAnalyzer Cloud**
- **FortiConverter Service**
- **IPAM Cloud**
- **SD-WAN Orchestrator Entitlement**
- **SD-WAN Cloud Assisted Monitoring**
- **FortiManager Cloud**

#### License Details

- **FortiGuard Bundles**
- **FortiCare**: 360 Protection
- **Enterprise Protection**: 24x7
- **Unified Threat Protection**: 24x7
- **Threat Protection**: 24x7

### Notes

- **Order Information**: [Order Information](#) (202012)
- **Bundles**: [Bundles](#) (202012)
- **Copyright**: [Copyright](#) (202012)