The FortiGate 200E 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
- 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 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 to consolidate networking and security

Management
- Includes a 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>20 Gbps</td>
<td>2.2 Gbps</td>
<td>1.8 Gbps</td>
<td>1.2 Gbps</td>
<td>Multiple GE RJ45, GE SFP Slots</td>
</tr>
</tbody>
</table>

Refer to specification table for details
Deployment

Next Generation Firewall (NGFW)

- Reduce complexity by combining threat protection security capabilities into the single high-performance network security appliance
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual applications in your network traffic
- Delivers industry’s highest SSL inspection performance using industry-mandated ciphers while maximizing ROI
- 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 reduced WAN cost spending
- High-performance and cost-effective threat protection capabilities
- WAN Path Controller and Link Health Monitoring for better application performance
- Security Processor powered industry’s best IPsec VPN and SSL Inspection performance
- Simplified Management and Zero-Touch deployment
**Hardware**

FortiGate 200E/201E

---

**Interfaces**

1. Console Port
2. USB Port
3. 2x GE RJ45 Management/HA Ports
4. 2x GE RJ45 WAN Ports
5. 14x GE RJ45 Ports
6. 4x GE SFP Slots

---

**Powered by SPU**

- 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

---

**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

---

**Network Processor**

The SPU NP6Lite network processor works inline with firewall and VPN functions delivering:

- Wire-speed firewall performance for any size packets
- VPN acceleration
- Anomaly-based intrusion prevention, checksum offload and packet defragmentation
- Traffic shaping and priority queuing
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 to deliver 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 200E</th>
<th>FORTIGATE 201E</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE RJ45 WAN Interfaces</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>GE RJ45 Management/HA Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GE RJ45 Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GE SFP Slots</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>USB port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Console (RJ45)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Storage</td>
<td>1x 480 GB SSD</td>
<td></td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

System Performance — Enterprise Traffic Mix

<table>
<thead>
<tr>
<th>IPS Throughput</th>
<th>2.2 Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Throughput</td>
<td>1.8 Gbps</td>
</tr>
<tr>
<td>Threat Protection Throughput</td>
<td>1.2 Gbps</td>
</tr>
</tbody>
</table>

System Performance

<table>
<thead>
<tr>
<th>Firewall Throughput (1518 / 512 / 84 byte UDP packets)</th>
<th>20 / 20 / 9 Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput (Packets Per Second)</td>
<td>200,000</td>
</tr>
<tr>
<td>Concurrent Sessions (TCP)</td>
<td>10,000</td>
</tr>
<tr>
<td>New Sessions/Second (TCP)</td>
<td>10,000</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>10,000</td>
</tr>
<tr>
<td>IPSec VPN Throughput</td>
<td>2.2 Gbps</td>
</tr>
<tr>
<td>Gateway-to-Gateway IPSec VPN Tunnels</td>
<td>1,000</td>
</tr>
<tr>
<td>Client-to-Gateway IPSec VPN Tunnels</td>
<td>10,000</td>
</tr>
<tr>
<td>SSL-IPsec Throughput</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>Concurrent SSL-VPN Users</td>
<td>500</td>
</tr>
</tbody>
</table>

SSL Inspection Throughput (IPS, avg. HTTPS) | 820 Mbps |

SSL Inspection CPS (IPS, avg. HTTPS) | 1000 |

SSL Inspection Concurrent Session (IPS, avg. HTTPS) | 240,000 |

Application Control Throughput (HTTP 64K) | 100 Mbps |

CAPN/APP Throughput (444 byte, UDP) | 15 Mbps |

Virtual Domains (Default / Maximum) | 10 / 10 |

Maximum Number of FortiSwitches Supported | 10 |

Maxumum Number of FortiAPs (Total / Tunnel Mode) | 128 / 64 |

Maxumum Number of FortiTokens | 5,000 |

Maxumum Number of Registered FortiClients | 600 |

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

1. IPSec VPN performance test uses AES256-SHA256.
2. 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

Product | SKU  | Description
--- | --- | ---
FortiGate 200E | FG-200E | 18x GE RJ45 (including 2x WAN ports, 1x Mgmt port, 1x HA port, 14x switch ports), 4x GE SFP slots, SPU NPULite and CP9 hardware accelerated.
FortiGate 201E | FG-201E | 18x GE RJ45 (including 2x WAN ports, 1x Mgmt port, 1x HA port, 14x switch ports), 4x GE SFP slots, SPU NPULite and CP9 hardware accelerated, 480 GB onboard SSD storage.

Optional Accessories


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>UTM</th>
<th>Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</td>
<td>ASE 1</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 Web Filtering Service</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>FortiGuard Antispam 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>FortiCASB SaaS-only 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>SD-WAN Cloud Assisted Monitoring 1</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>SD-WAN Overlay Controller VPN Service 1</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>FortiAnalyzer Cloud 1</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>FortiManager Cloud 1</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

1. 24x7 plus Advanced Services Ticket Handling  
2. Available when running FortiOS 6.2