The FortiGate 2200E series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across internal segments. Leverage industry-leading IPS, SSL inspection, and advanced threat protection to optimize your network’s performance. 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

Networks
- 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>158 Gbps</td>
<td>16.5 Gbps</td>
<td>13.5 Gbps</td>
<td>11 Gbps</td>
<td>Multiple GE RJ45, 10 GE SFP+, 25 GE SFP28, and 40 GE QSFP+ 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 security effectiveness, 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 advanced threat protection provided by the intelligence services of the Fortinet Security Fabric

Mobile Security for 4G, 5G, and IOT
- SPU accelerated, high performance CGNAT and IPv6 migration option including: NAT44, NAT444, NAT64/DNS64, NAT46 for 4G Gi/sGi and 5G N6 connectivity and security
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- 4G and 5G security for user and data plane traffic including SCTP, GTP-U and SLP that provides protection against attacks
- High-speed interfaces to enable deployment flexibility

Segmentation
- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns

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 URLs 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

IPS
- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric

Mobile Security for 4G, 5G, and IOT
- SPU accelerated, high performance CGNAT and IPv6 migration option including: NAT44, NAT444, NAT64/DNS64, NAT46 for 4G Gi/sGi and 5G N6 connectivity and security
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- 4G and 5G security for user and data plane traffic including SCTP, GTP-U and SLP that provides protection against attacks
- High-speed interfaces to enable deployment flexibility

Hardware

FortiGate 2200E/2201E

Interfaces
1. USB Port
2. 2x 1GE RJ45 MGMT Ports
3. 1x CONSOLE Port
4. 1xVPN Client Port
5. 18x 25 GE SFP28 / 10 GE SFP+ Slots
6. 2x 25 GE SFP28 / 10 GE SFP+ HA Slots
7. 4x 40 GE QSFP+ Slots
8. 12x 40 GbE Ports

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 the unique capability of full signature matching at SPU
- SSL Inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading

High-Speed Connectivity
High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 2200E series provides 40 GE and 25 GE interfaces, simplifying network designs without relying on additional devices to bridge desired connectivity.
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
FortiGate 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, and forti.net/fortiguard.
- 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:

**For more information, please refer to forti.net/fortiguard and forti.net/forticare**

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.

Specifications

**FortiGate 2200E**

- **Dimensions and Power**
  - Weight (Height x Width x Length): 53.0 x 17.4 x 17.0 (inches)
  - Weight (Height x Width x Length): 135 x 444 x 556 (millimeters)
- **Rack Mount, 2 RU**
- **Heat Dissipation**: 400 W
- **Noise Level**: 65 dBA
- **Humidity**: 9–90% non-condensing
- **Storage Temperature**: -31–158°F (-35–70°C)
- **Operating Temperature**: 32–104°F (0–40°C)
- **Power Consumption (Average / Maximum)**: 300 W / 650 W
- **Power Input**: 100–240V AC, 50–60 Hz
- **Redundant Power Supplies**: Yes, Hot swappable
- **Dimensions and Power**
  - **Heat Dissipation**: 400 W
  - **Noise Level**: 65 dBA
  - **Humidity**: 9–90% non-condensing
  - **Storage Temperature**: -31–158°F (-35–70°C)
  - **Operating Temperature**: 32–104°F (0–40°C)
  - **Power Consumption (Average / Maximum)**: 300 W / 650 W
  - **Power Input**: 100–240V AC, 50–60 Hz
  - **Redundant Power Supplies**: Yes, Hot swappable

**FortiGate 2201E**

- **Dimensions and Power**
  - Weight (Height x Width x Length): 53.0 x 17.4 x 17.0 (inches)
  - Weight (Height x Width x Length): 135 x 444 x 556 (millimeters)
- **Rack Mount, 2 RU**
- **Heat Dissipation**: 400 W
- **Noise Level**: 65 dBA
- **Humidity**: 9–90% non-condensing
- **Storage Temperature**: -31–158°F (-35–70°C)
- **Operating Temperature**: 32–104°F (0–40°C)
- **Power Consumption (Average / Maximum)**: 300 W / 650 W
- **Power Input**: 100–240V AC, 50–60 Hz
- **Redundant Power Supplies**: Yes, Hot swappable

**For more information, please refer to forti.net/fortiguard and forti.net/forticare**

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

1. AV performance is measured in USGv6/IPv6.
2. IPS, Intrusion Prevention System, and Firewalls are measured with Log and Alerting enabled.
3. AVG performance is measured on the following TPS versions of different cipher suites:
   - TPS versions of different cipher suites:
   - [Fortinet Security Fabric](#)
   - [FortiOS](#)
   - [FortiGuard](#)
   - [FortiCare](#)
   - [FortiGuard](#)
   - [FortiCare](#)
   - [FortiGuard](#)
   - [FortiCare](#)

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

FortiGate 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.

- **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 within minutes with an integrated AI-driven security and advanced threat protection.**
- **Leverage the latest technologies such as deception-based security and advanced threat protection.**
- **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.

For more information, please refer to forti.net/fortiguard and forti.net/forticare
DATA SHEET | FortiGate® 2200E Series

Order Information

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 2200E</td>
<td>FG-2200E</td>
<td>4x 40 GE SFP+ = slots, 20x 25 GE SFP28 slots (including 18x ports, 2x HA ports), 1x4 GE RJ45 ports (including 1x ports, 2x management port), SPU NPA and CP9 hardware accelerated, and dual AC power supplies.</td>
</tr>
<tr>
<td>FortiGate 2201E</td>
<td>FG-2201E</td>
<td>4x 40 GE SFP+ = slots, 20x 25 GE SFP28 slots (including 18x ports, 2x HA ports), 1x4 GE RJ45 ports (including 1x ports, 2x management port), SPU NPA and CP9 hardware accelerated, and dual AC power supplies, with 2x 1 TB SSD onboard storage.</td>
</tr>
</tbody>
</table>

Optional Accessories/Spares

<table>
<thead>
<tr>
<th>10 GE SFP+ Transceiver Module, Short Range</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FG-TRAN-SFP+SR</td>
<td></td>
<td>10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>FG-TRAN-SFP+LR</td>
<td></td>
<td>10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>40 GE QSFP+ Transceivers</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FG-TRAN-QSFP+SR-BIDI</td>
<td></td>
<td>40 GE QSFP+ transceivers, short range BiDi for systems with QSFP+ slots.</td>
</tr>
<tr>
<td>FG-TRAN-QSFP+LR</td>
<td></td>
<td>40 GE QSFP+ transceivers, long range for all systems with QSFP+ slots.</td>
</tr>
</tbody>
</table>

Rack Mount Sliding Rails

<table>
<thead>
<tr>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
</table>

AC Power Supply

<table>
<thead>
<tr>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-FG3800D-PS</td>
<td>AC power supply for FG-2200/2201E, FG-3300/3301E, FG-3400/3401E, FG-3600/3601E, FG-3700D, FG-3700D-NEBS, FG-3700DX, FG-3810D and FG-3815D.</td>
</tr>
</tbody>
</table>

Bundles

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.

<table>
<thead>
<tr>
<th>Bundles</th>
<th>360 Protection</th>
<th>Enterprise Protection</th>
<th>Unified Threat Protection</th>
<th>Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</td>
<td>ASE/24x7/24x7</td>
<td>24x7/24x7</td>
<td>24x7/24x7</td>
<td>24x7/24x7</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>FortiGuard IoT Detection Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiConvert Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPAM Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Orchestrator Entitlement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Cloud Assisted Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Overlay Controller VPN Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiAnalyzer Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiManager Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. 24x7 plus Advanced Services Ticket Handling  2. Available when running FortiOS 6.4