

# FortiGate® 2200E Series

FG-2200E and 2201E

Next Generation Firewall  
Segmentation  
Secure Web Gateway  
IPS  
Mobile Security



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, ICASA, Virus Bulletin, and AV Comparatives

### Networking

- 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

Firewall	IPS	NGFW	Threat Protection	Interfaces
<b>158 Gbps</b>	<b>16.5 Gbps</b>	<b>13.5 Gbps</b>	<b>11 Gbps</b>	Multiple GE RJ45, 10 GE SFP+, 25 GE SFP28, and 40 GE QSFP+ slots

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 AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric



### 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 URL's 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



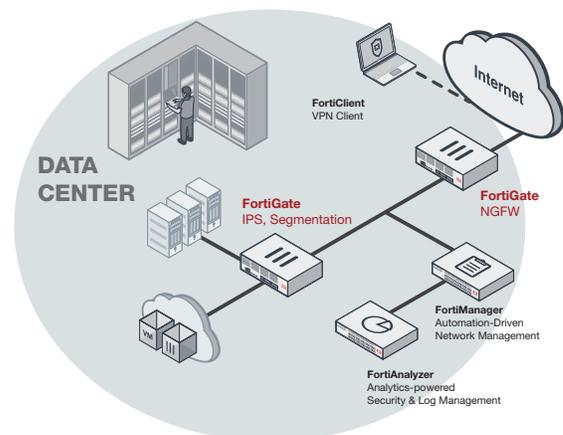
### IPS

- 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

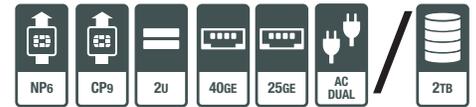
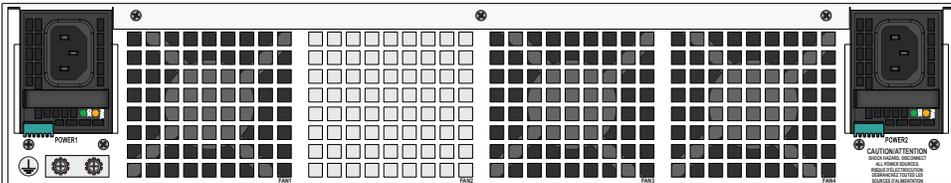
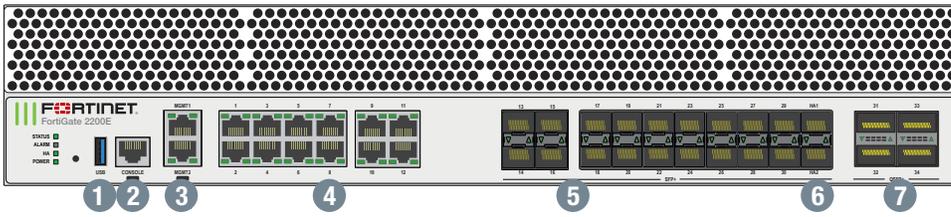
- SPU accelerated, high performance CGNAT and IPv6 migration option including: NAT44, NAT444, NAT64/DNS64, NAT46 for 4G Gi/sGi and 5G N6 connectivity and security
- RAN Access Security with highly scalable and best performing IPsec aggregation and control security gateway (SecGW)
- User plane security 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 SIP that provides protection against attacks
- High-speed interfaces to enable deployment flexibility



FortiGate 2200E deployment in data center  
(NGFW, IPS, and Intent-based Segmentation)

# Hardware

## FortiGate 2200E/2201E



## Interfaces

- |  |   |
|--|---|
| <ol style="list-style-type: none"> <li>1. USB Port</li> <li>2. Console Port</li> <li>3. 2x GE RJ45 MGMT Ports</li> <li>4. 12x GE RJ45 Ports</li> </ol> | <ol style="list-style-type: none"> <li>5. 18x 25 GE SFP28 / 10 GE SFP+ Slots</li> <li>6. 2x 25 GE SFP28 / 10 GE SFP+ HA Slots</li> <li>7. 4x 40 GE QSFP+ Slots</li> </ol> |
|--|---|

### Powered by SPU

- Custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck



### 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

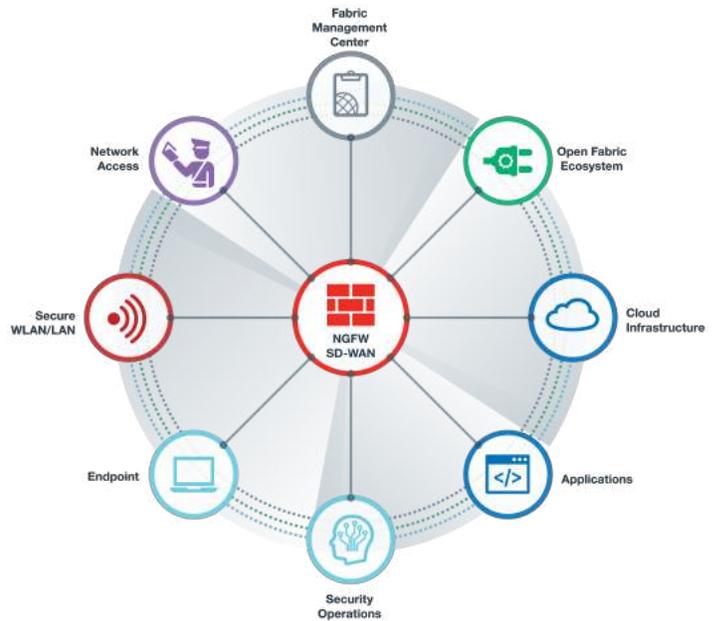
High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 2200E series provides 40 GE and 25 GE interfaces, simplifying network designs without relying on additional devices to bridge desired connectivity.

# 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

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 ICSCA validated security and performance.
- Leverage the latest technologies such as deception-based 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.

- 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.



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](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)

# Specifications

	FORTIGATE 2200E	FORTIGATE 2201E
<b>Interfaces and Modules</b>		
Hardware Accelerated 40 GE QSFP+ Slots		4
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ HA Slots		2
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ Slots		18
Hardware Accelerated GE RJ45 Ports		12
GE RJ45 Management Ports		2
USB Port		1
Console Port		1
Onboard Storage	–	2x 1 TB SSD
Included Transceivers		2x SFP+ (SR 10 GE)
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		16.5 Gbps
NGFW Throughput <sup>2,4</sup>		13.5 Gbps
Threat Protection Throughput <sup>2,5</sup>		11 Gbps
<b>System Performance and Capacity</b>		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)		158 / 155 / 100 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)		158 / 155 / 100 Gbps
Firewall Latency (64 byte, UDP)		4 µs
Firewall Throughput (Packet per Second)		150 Mpps
Concurrent Sessions (TCP)		24 Million
New Sessions/Second (TCP)		500,000
Firewall Policies		100,000
IPsec VPN Throughput (512 byte) <sup>1</sup>		98 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		20,000
Client-to-Gateway IPsec VPN Tunnels		100,000
SSL-VPN Throughput		10 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>		17 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>		9,500
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>		2.5 Million
Application Control Throughput (HTTP 64K) <sup>2</sup>		52 Gbps
CAPWAP Throughput (HTTP 64K)		60 Gbps
Virtual Domains (Default / Maximum)		10 / 500
Maximum Number of FortiSwitches Supported		196
Maximum Number of FortiAPs (Total / Tunnel)		4,096 / 2,048
Maximum Number of FortiTokens		20,000
High Availability Configurations		Active-Active, Active-Passive, Clustering

	FORTIGATE 2200E	FORTIGATE 2201E
<b>Dimensions and Power</b>		
Height x Width x Length (inches)	3.5 x 17.44 x 21.89	
Height x Width x Length (mm)	88.9 x 443 x 556	
Weight	40.0 lbs (18.2 kg)	41.4 lbs (18.8 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2 RU	
Power Input	100–240V AC, 50–60 Hz	
Power Consumption (Average / Maximum)	408 W / 571 W	412 W / 577 W
Current (Maximum)	12A@100V, 9A@240V	
Heat Dissipation	1948 BTU/h	1968 BTU/h
Redundant Power Supplies	Yes, Hot swappable	
<b>Operating Environment and Certifications</b>		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	70 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6	

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.

## Order Information

Product	SKU	Description
FortiGate 2200E	FG-2200E	4x 40 GE QSFP+ slots, 20x 25 GE SFP28 slots (including 18x ports, 2x HA ports), 14x GE RJ45 ports (including 12x ports, 2x management ports), SPU NP6 and CP9 hardware accelerated, and dual AC power supplies.
FortiGate 2201E	FG-2201E	4x 40 GE QSFP+ slots, 20x 25 GE SFP28 slots (including 18x ports, 2x HA ports), 14x GE RJ45 ports (including 12x ports, 2x management ports), SPU NP6 and CP9 hardware accelerated, and dual AC power supplies, with 2x 1 TB SSD onboard storage.
Optional Accessories/Spares	SKU	Description
10 GE SFP+ Transceiver Module, Short Range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.
25 GE SFP28 Transceiver Module, Long Range	FG-TRAN-SFP28-LR	25 GE SFP28 transceiver module, long range for all systems with SFP28 slots.
25 GE/10 GE Dual Rate SFP28 Transceiver Module, Short Range	FG-TRAN-SFP28-SR	25 GE/10 GE dual rate SFP28 transceiver module, short range for all systems with SFP28/SFP+ slots.
40 GE QSFP+ Transceivers, Short Range	FG-TRAN-QSFP+SR	40 GE QSFP+ transceivers, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceivers, Short Range, BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceivers, short range BiDi for systems with QSFP+ slots.
40 GE QSFP+ Transceivers, Long Range	FG-TRAN-QSFP+LR	40 GE QSFP+ transceivers, long range for all systems with QSFP+ slots.
40 GE QSFP+ to 4x 10GE SFP+ Optical Breakout	FG-TRAN-QSFP+4XSFP	40GE QSFP+ Parallel Breakout Active Optical Cable with 1m length for all systems with QSFP+ slots.
QSFP+ to 4xSFP+ Optical breakout 5m	FG-TRAN-QSFP+4SFP-5	40G QSFP+ Parallel Breakout MPO to 4xLC connectors, 5m reach, transceivers not included.
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1100/1101E, FG-1200D, FG-1500D/-DC, FG-2000E, FG-2200E/2201E, FG-2500E, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3300E/3301E, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC and FG-3950B/-DC.
AC Power Supply	SP-FG3800D-PS	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.

## 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.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Threat Protection
FortiCare	ASE <sup>1</sup>	24x7	24x7	24x7
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 <sup>2</sup>	•	•		
FortiConverter Service	•	•		
IPAM Cloud <sup>2</sup>	•			
SD-WAN Orchestrator Entitlement <sup>2</sup>	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

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