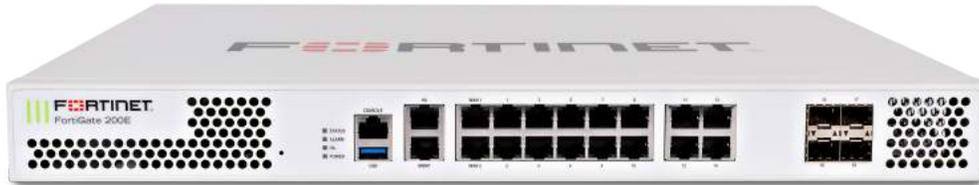**FORTINET**

FortiGate® 200E Series

FortiGate 200E and 201E

Next Generation Firewall
Secure SD-WAN
Secure Web Gateway

The FortiGate 200E series delivers next generation firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or enterprise branch level. Protects against cyber threats with high-powered security processors for optimized network performance, security efficacy and deep visibility. 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

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
20 Gbps	**2.2 Gbps**	**1.8 Gbps**	**1.2 Gbps**	Multiple GE RJ45, GE SFP Slots

Refer to the specifications table for details
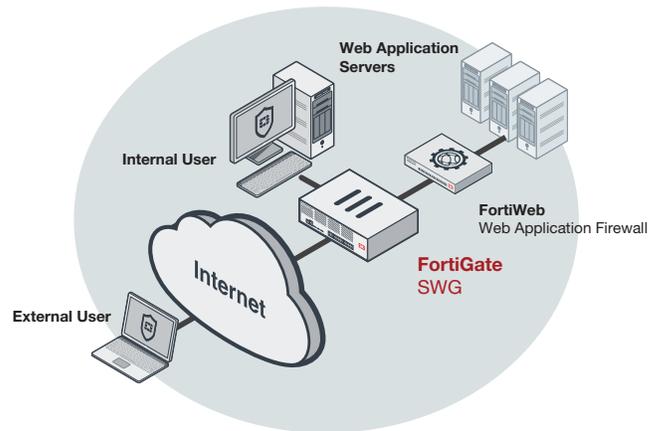
Deployment

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 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
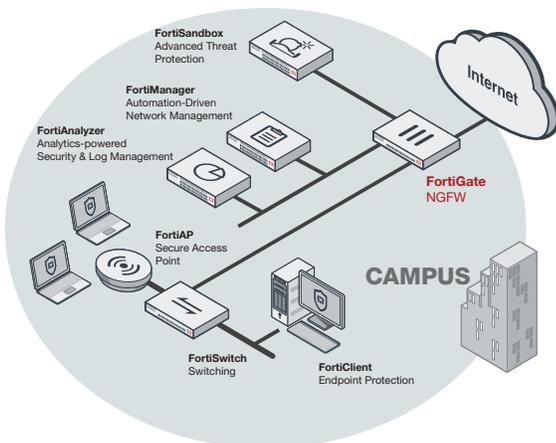
Secure SD-WAN

- Consistent business application performance with accurate detection, dynamic WAN path steering and optimization
- Multi-cloud access for faster SaaS adoption with end-to-end optimization
- Simplification with zero touch deployment and centralized management with auto-provisioning, analytics and reporting
- Strong security posture with next generation firewall and real-time threat protection

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
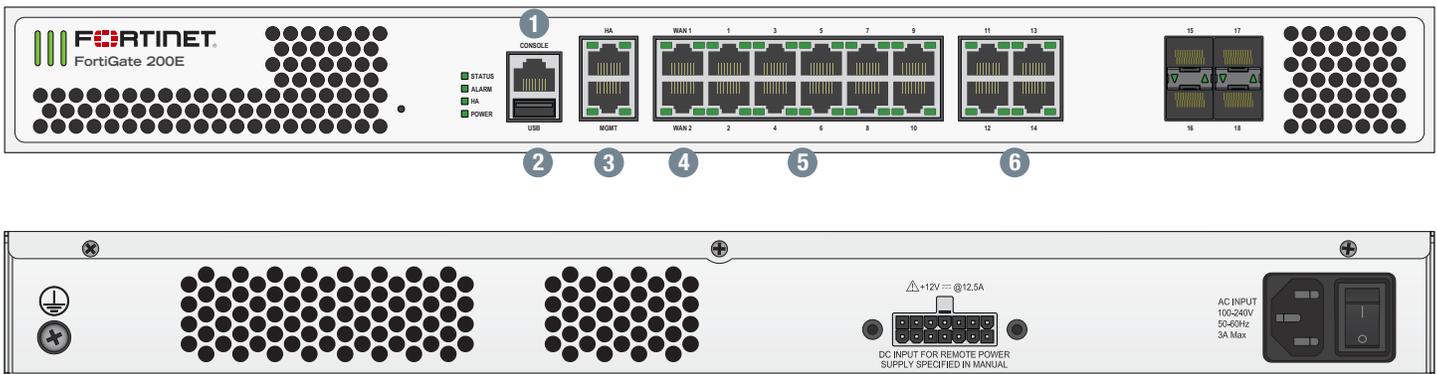

FortiGate 200E SWG deployment

FortiGate 200E deployment in Campus
(NGFW)
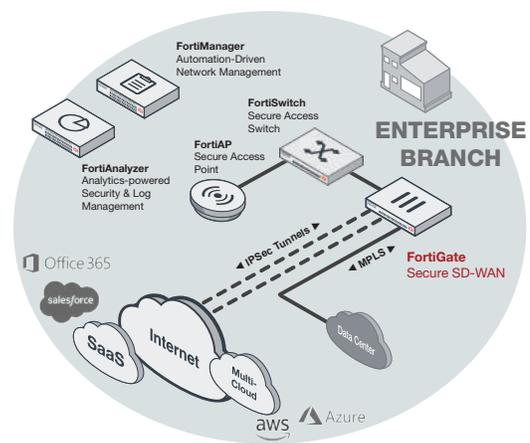
FortiGate 200E deployment in Enterprise Branch
(Secure SD-WAN)

F⊟RTINET

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

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 and 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 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 overs 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
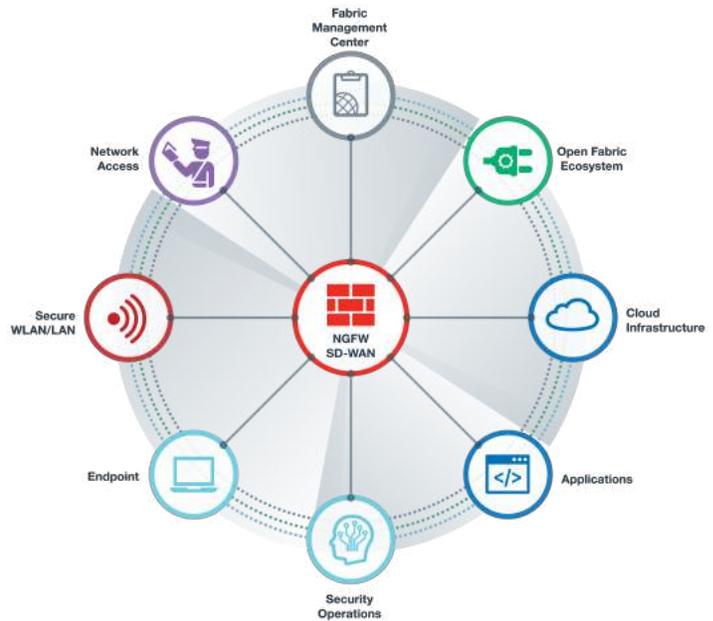
FortiOS

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

F⊟RTINET

Specifications

	FORTIGATE 200E	FORTIGATE 201E
Hardware Specifications		
GE RJ45 WAN Interfaces	2	
GE RJ45 Management/HA Ports	2	
GE RJ45 Ports	14	
GE SFP Slots	4	
USB port	1	
Console (RJ45)	1	
Local Storage	—	1x 480 GB SSD
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	2.2 Gbps	
NGFW Throughput [2, 4]	1.8 Gbps	
Threat Protection Throughput [2, 5]	1.2 Gbps	
System Performance		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	20 / 20 / 9 Gbps	
Firewall Latency (64 byte UDP packets)	3 µs	
Firewall Throughput (Packets Per Second)	13.5 Mpps	
Concurrent Sessions (TCP)	2 Million	
New Sessions/Second (TCP)	135,000	
Firewall Policies	10,000	
IPsec VPN Throughput (512 byte) [1]	7.2 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2,000	
Client-to-Gateway IPsec VPN Tunnels	10,000	
SSL-VPN Throughput	900 Mbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	820 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	1,000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	240,000	
Application Control Throughput (HTTP 64K) [2]	3.5 Gbps	
CAPWAP Throughput (1444 byte, UDP)	1.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	64	
Maximum Number of FortiAPs (Total / Tunnel Mode)	256 / 128	
Maximum Number of FortiTokens	5,000	
High Availability Configurations	Active / Active, Active / Passive, Clustering	

	FORTIGATE 200E	FORTIGATE 201E
Dimensions		
Height x Width x Length (inches)	1.75 x 17.0 x 11.9	
Height x Width x Length (mm)	44.45 x 432 x 301	
Weight	11.9 lbs (5.4 kg)	12.12 lbs (5.5 kg)
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 1 RU	
Environment		
Power Input	100–240V AC, 50–60 Hz	
Maximum Current	110 V / 3 A, 220 V / 0.42 A	
Power Consumption (Average / Maximum)	70.98 / 109.9 W	
Heat Dissipation	374.9 BTU/h	
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	31.1 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; 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 200E	FG-200E	18x GE RJ45 (including 2x WAN ports, 1x Mgmt port, 1x HA port, 14x switch ports), 4x GE SFP slots. SPU NP6Lite 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 NP6Lite and CP9 hardware accelerated, 480 GB onboard SSD storage.
Optional Accessories		
External redundant AC power supply	FRPS-100	External redundant AC power supply for up to 4 units: FG-100/101E, FG-300C, FG-310B, FS-348B and FS-448B. Up to 2 units: FG-200B, FG-200D, FG-200/201E, FG-240D and FG-300D, FG-400D, FG-500D, FG-600D, FHV-500D, FDD-200B, FDD-400B, FDD-600B and FDD-800B.
1 GE SFP LX transceiver module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 transceiver module	FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX transceiver module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.

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 [1]	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 [2]	•	•		
FortiConverter Service	•	•		
IPAM Cloud [2]	•			
SD-WAN Orchestrator Entitlement [2]	•			
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