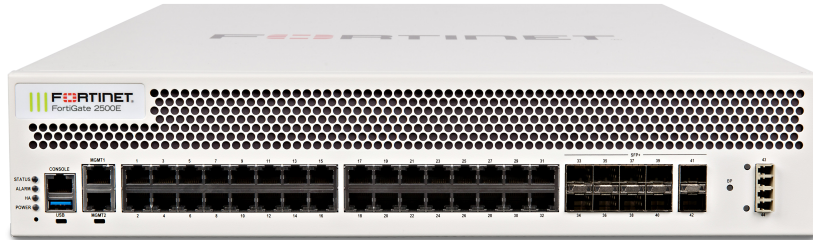


FortiGate® 2500E

FG-2500E

**Next Generation Firewall
Segmentation
Secure Web Gateway
IPS
Mobile Security**



The FortiGate 2500E 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
- Prevent and detect 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 for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet’s 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

| Firewall | IPS | NGFW | Threat Protection | Interfaces |
|----------|-----------|--------|-------------------|--|
| 150 Gbps | 11.5 Gbps | 9 Gbps | 5.4 Gbps | Multiple GE RJ45, 10 GE SFP+ slots and Bypass 10 GE SFP+ ports |

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



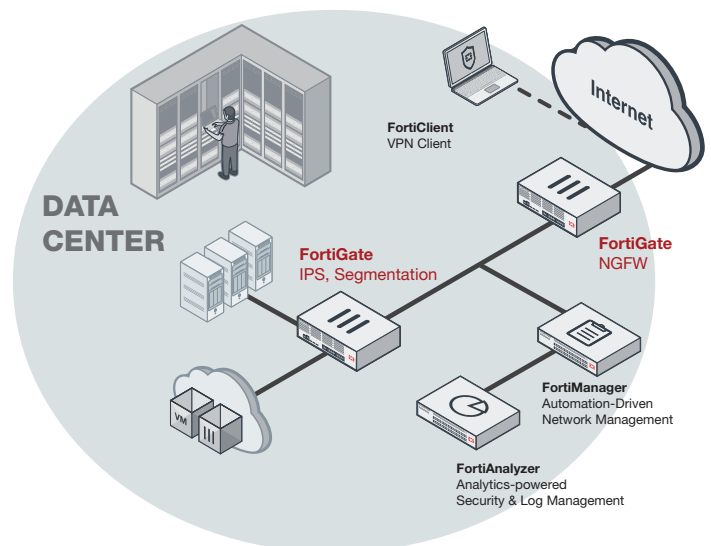
IPS

- 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

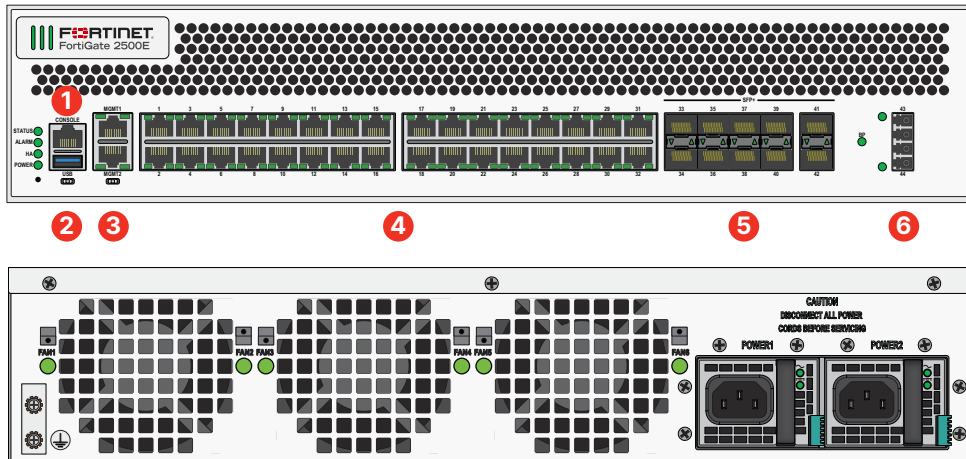


**Data Center Deployment
(NGFW, IPS, and Intent-based Segmentation)**



HARDWARE

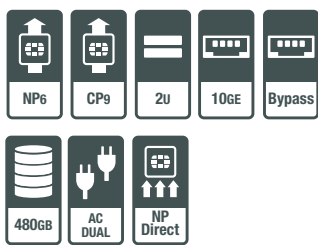
FortiGate 2500E



Interfaces

1. Console Port
2. USB Port
3. 2x GE RJ45 Management Ports
4. 32x GE RJ45 Ports
5. 10x 10 GE SFP+ Slots
6. 2x 10 GE SFP+ SR (LC Connector, bypass)

Hardware Features



NP Direct

By removing the Internal Switch Fabric, the NP Direct architecture provides direct access to the SPU-NP for the lowest latency forwarding. NGFW deployments require some attention to network design to ensure optimal use of this technology.

Powered by SPU

- Fortinet’s 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
- VPN, CAPWAP and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

Fortinet’s ninth generation custom SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection.

High-Speed 10 GE Connectivity

High speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 2500E provides high 10 GE port densities, simplifying network designs without relying on additional devices to bridge desired connectivity.



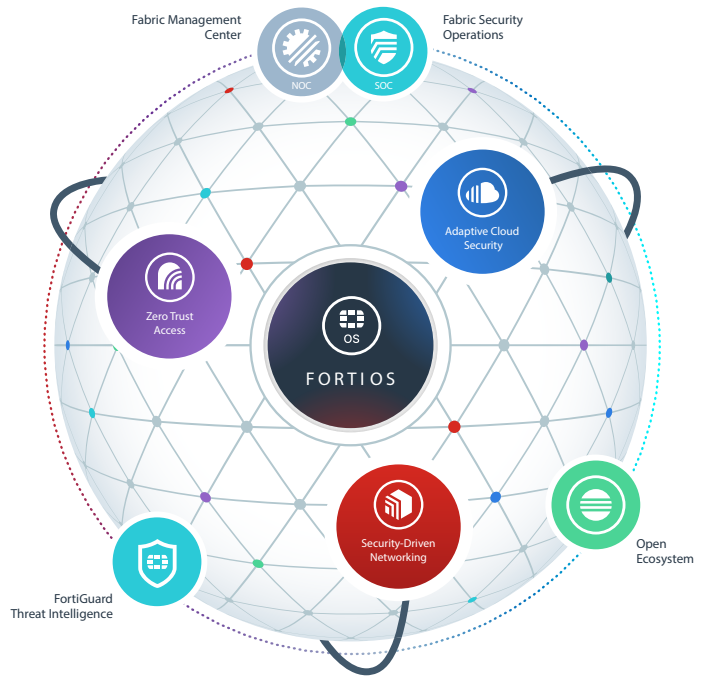
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad:** Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated:** Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated:** Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models consisting on appliances, software and As-a-Service with SASE, ZTNA and other emerging cybersecurity solutions.

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™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1,000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.



SPECIFICATIONS

| FORTIGATE 2500E | |
|--|---|
| Interfaces and Modules | |
| Hardware Accelerated 10 GE SFP+ Slots | 10 + 2 bypass |
| Hardware Accelerated GE RJ45 Ports | 32 |
| GE RJ45 Management / HA Ports | 2 |
| USB Ports | 1 |
| Console Port | 1 |
| Internal Storage | 1x 480 GB SSD |
| Included Transceivers | 2x SFP+ (SR 10GE) |
| System Performance — Enterprise Traffic Mix | |
| IPS Throughput ² | 11.5 Gbps |
| NGFW Throughput ^{2,4} | 9 Gbps |
| Threat Protection Throughput ^{2,5} | 5.4 Gbps |
| System Performance and Capacity | |
| IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) | 150 / 150 / 95 Gbps |
| IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) | 150 / 150 / 95 Gbps |
| Firewall Latency (64 byte, UDP) | 2.00 µs |
| Firewall Throughput (Packet per Second) | 145.5 Mpps |
| Concurrent Sessions (TCP) | 20 Million |
| New Sessions/Second (TCP) | 500,000 |
| Firewall Policies | 100,000 |
| IPsec VPN Throughput (512 byte) ¹ | 95 Gbps |
| Gateway-to-Gateway IPsec VPN Tunnels | 20,000 |
| Client-to-Gateway IPsec VPN Tunnels | 100,000 |
| SSL-VPN Throughput | 6 Gbps |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | 30,000 |
| SSL Inspection Throughput (IPS, avg. HTTPS) ³ | 9.4 Gbps |
| SSL Inspection CPS (IPS, avg. HTTPS) ³ | 5,500 |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³ | 2 Million |
| Application Control Throughput (HTTP 64K) ² | 20 Gbps |
| CAPWAP Throughput (1444 byte, UDP) | 21 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 2500E | |
|---|---|
| Dimensions and Power | |
| Height x Width x Length (inches) | 3.5 x 17.4 x 21.9 |
| Height x Width x Length (mm) | 88 x 442 x 555 |
| Weight | 38.5 lbs (17.6 kg) |
| Form Factor (supports EIA/non-EIA standards) | Rack Mount, 2 RU |
| Power | |
| Power Input | 100-240V AC, 50/60 Hz |
| Maximum Current | 9A |
| Power Consumption (Average / Maximum) | 312 W / 470 W |
| Heat Dissipation | 1,604 BTU/h |
| Redundant Power Supplies | Yes, Hot Swappable |
| Operating Environment and Certifications | |
| Operating Temperature | 32-104°F (0-40°C) |
| Storage Temperature | -31-158°F (-35-70°C) |
| Humidity | 10-90% non-condensing |
| Noise Level | 58 dBA |
| Forced Airflow | Front to Back |
| 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 |

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.



ORDERING INFORMATION

| Product | SKU | Description |
|--|------------------|---|
| FortiGate 2500E | FG-2500E | 10x 10 GE SFP+ slots, 2x 10 GE bypass SFP+ (LC Adapter), 34x GE RJ45 ports (including 32x ports, 2x management/HA ports), SPU NP6 and CP9 hardware accelerated, 480 GB SSD onboard storage. |
| Optional Accessories | | |
| 10 GE SFP+ RJ45 Transceiver Module | FN-TRAN-SFP+GC | 10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots. |
| 10 GE SFP+ Transceiver Module, Short Range | FN-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 | FN-TRAN-SFP+LR | 10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots. |
| 10 GE SFP+ Transceiver Module, Extended Range | FN-TRAN-SFP+ER | 10 GE SFP+ transceiver module, extended 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. |
| Rack Mount Sliding Rails | SP-FG3040B-RAIL | Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D/DC, FG-2000E, FG-2500E, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC, FG-3815D/-DC and FG-3950B/-DC. |
| AC Power Supply | SP-FG2000E-PS | AC power supply for FG-2000E and FG-2500E. |

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 | Enterprise Protection | Unified Threat Protection | Advanced Threat Protection |
|---|-----------------------|---------------------------|----------------------------|
| FortiCare | 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 and Video ¹ Filtering Service | • | • | |
| FortiGuard Antispam Service | • | • | |
| FortiGuard Security Rating Service | • | | |
| FortiGuard IoT Detection Service | • | | |
| FortiGuard Industrial Service | • | | |
| FortiConverter Service | • | | |

1. Available when running FortiOS 7.0



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.