

FortiGate® 600E Series

FortiGate 600E and 601E

 Next Generation Firewall
Secure SD-WAN
Secure Web Gateway
IPS


The FortiGate 600E series provides an application-centric, scalable, and secure SD-WAN solution with Next Generation Firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or branch level. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. 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

- Dynamic path selection over any WAN transport to provide better application experience based on self-healing SD-WAN capabilities
- Advanced routing, scalable VPN, multi-cast, and IPV4/IPV6 forwarding powered by purpose-built network processors

Management

- SD-WAN orchestration provides intuitive and simplified workflow for centralized management and provisioning of business policies in a few easy clicks
- Expedited deployment with zero touch provisioning well-suited for large and distributed infrastructure
- Automated VPN tunnels for flexible hub-to-spoke and full-mesh deployment at scale to provide bandwidth aggregation and encrypted WAN paths
- 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 |
|----------|---------|----------|-------------------|---|
| 36 Gbps | 10 Gbps | 9.5 Gbps | 7 Gbps | Multiple GE RJ45, GE SFP and 10 GE SFP+ Slots |

Refer to the specifications table for details

Deployment



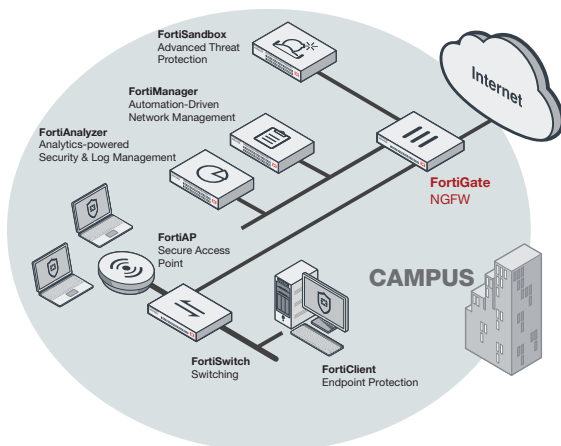
Next Generation Firewall (NGFW)

- 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, and 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 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



FortiGate 600E deployment in Campus (NGFW)



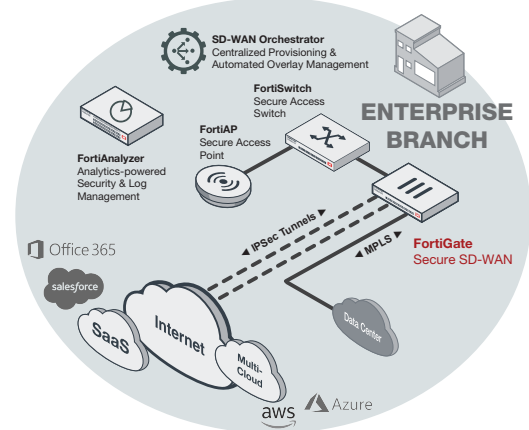
Secure SD-WAN

- Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport
- Accelerated multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based and real-time bandwidth compute-based traffic steering
- Automated overlay tunnels provides encryption and abstracts physical hybrid WAN making it simple to manage.
- Simplified and intuitive workflow with SD-WAN orchestrator for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identifies anomalies
- Strong security posture with next generation firewall and real-time threat protection



IPS

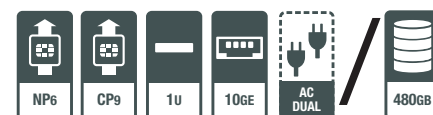
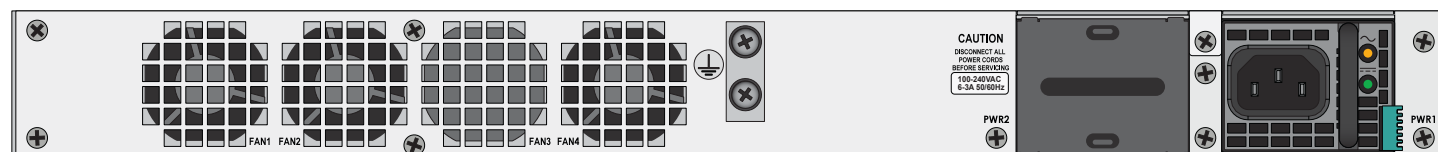
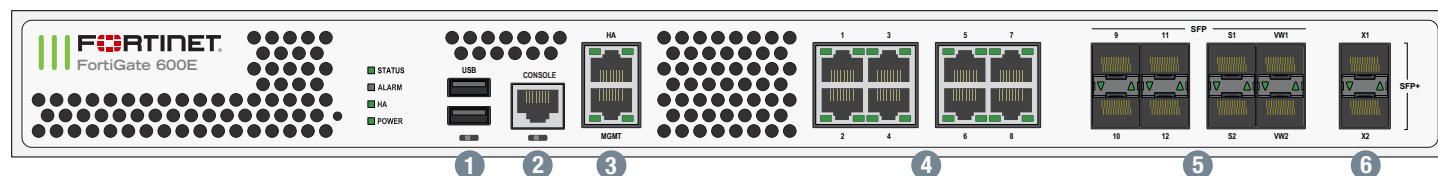
- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers 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



FortiGate 600E deployment in Enterprise Branch (Secure SD-WAN)

Hardware

FortiGate 600E/601E



Interfaces

- (1) 1x USB Port
- (2) 1x Console Port
- (3) 2x GE RJ45 MGMT/HA Ports

- (4) 8x GE RJ45 Ports
- (5) 8x GE SFP Slots
- (6) 2x 10 GE SFP+ Slots

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 two 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:

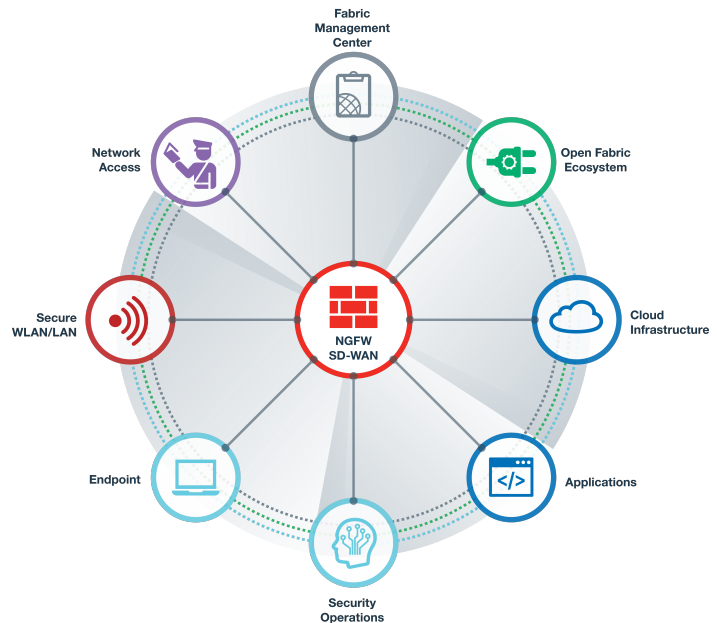
- Enhanced IPS performance with unique capability of full signature matching at ASIC
- SSL inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading

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 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

- 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

Specifications

| | FORTIGATE 600E | FORTIGATE 601E |
|---|---|----------------|
| Interfaces and Modules | | |
| 10 GE SFP+ Slots | 2 | |
| GE RJ45 Interfaces | 8 | |
| GE SFP Slots | 8 | |
| GE RJ45 Management Ports | 2 | |
| USB Ports | 2 | |
| RJ45 Console Port | 1 | |
| Local Storage | — | 2x 240 GB SSD |
| Included Transceivers | 2x SFP (SX 1 GE) | |
| System Performance — Enterprise Traffic Mix | | |
| IPS Throughput ² | 10 Gbps | |
| NGFW Throughput ^{2,4} | 9.5 Gbps | |
| Threat Protection Throughput ^{2,5} | 7 Gbps | |
| System Performance and Capacity | | |
| IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) | 36 / 36 / 27 Gbps | |
| IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP) | 36 / 36 / 27 Gbps | |
| Firewall Latency (64 byte, UDP) | 1.54 µs | |
| Firewall Throughput (Packet per Second) | 40.5 Mpps | |
| Concurrent Sessions (TCP) | 8 Million | |
| New Sessions/Second (TCP) | 450,000 | |
| Firewall Policies | 10,000 | |
| IPsec VPN Throughput (512 byte) ¹ | 20 Gbps | |
| Gateway-to-Gateway IPsec VPN Tunnels | 2,000 | |
| Client-to-Gateway IPsec VPN Tunnels | 50,000 | |
| SSL-VPN Throughput | 7 Gbps | |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | 10,000 | |
| SSL Inspection Throughput (IPS, avg. HTTPS) ³ | 8 Gbps | |
| SSL Inspection CPS (IPS, avg. HTTPS) ³ | 5,500 | |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³ | 800,000 | |
| Application Control Throughput (HTTP 64K) ² | 15 Gbps | |
| CAPWAP Throughput (HTTP 64K) | 18 Gbps | |
| Virtual Domains (Default / Maximum) | 10 / 10 | |
| Maximum Number of FortiSwitches Supported | 96 | |
| Maximum Number of FortiAPs (Total / Tunnel) | 1,024 / 512 | |
| Maximum Number of FortiTokens | 5,000 | |
| High Availability Configurations | Active-Active, Active-Passive, Clustering | |

| | FORTIGATE 600E | FORTIGATE 601E |
|---|--|-------------------|
| Dimensions and Power | | |
| Height x Width x Length (inches) | 1.75 x 17.0 x 15.0 | |
| Height x Width x Length (mm) | 44.45 x 432 x 380 | |
| Weight | 16.1 lbs (7.3 kg) | 16.6 lbs (7.5 kg) |
| Form Factor (supports EIA / non-EIA standards) | Rack Mount, 1 RU | |
| Power Consumption (Average / Maximum) | 129 W / 244 W | |
| Power Source | 100–240V 50–60Hz | |
| Current (Maximum) | 6A @ 100V | |
| Heat Dissipation | 832 BTU/h | |
| Redundant Power Supplies (Hot Swappable) | optional | |
| 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 | 59 dBA | |
| Operating Altitude | Up to 9,843 ft (3,000 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 600E | FG-600E | 2x 10 GE SFP+ slots, 10x GE RJ45 ports (including 1x MGMT port, 1x HA port, 8x switch ports), 8x GE SFP slots, SPU NP6 and CP9 hardware accelerated. |
| FortiGate 601E | FG-601E | 2x 10 GE SFP+ slots, 10x GE RJ45 ports (including 1x MGMT port, 1x HA port, 8x switch ports), 8x GE SFP slots, SPU NP6 and CP9 hardware accelerated, 2x 240 GB onboard SSD storage. |
| Optional Accessories | | |
| 1 GE SFP LX Transceiver Module | FN-TRAN-LX | 1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1 GE SFP RJ45 Transceiver Module | FN-TRAN-GC | 1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1 GE SFP SX Transceiver Module | FN-TRAN-SX | 1 GE SFP SX transceiver module for all systems with SFP and SFP/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, 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+ RJ45 Transceiver Module | FN-TRAN-SFP+GC | 10 GE SFP+ RJ45 transceiver module for systems with 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. |
| Optional Power Supply | SP-FG300E-PS | AC power supply for FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FAZ-200F/300F/800F and FMG-200F/300F. |

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



www.fortinet.com

Copyright © 2020 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. 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.