# FortiGate® 3600E Series

FG-3600E/-DC and 3601E
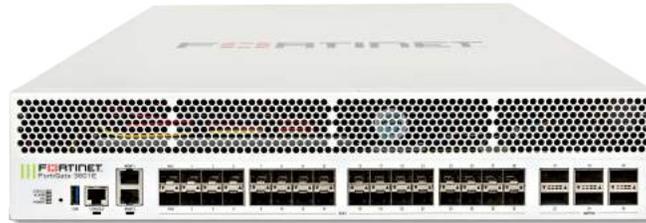
The FortiGate 3600E series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across 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

## 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 |
|---|---|---|---|---|
| 240 Gbps | 55 Gbps | 40 Gbps | 30 Gbps | Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP and 100 GE QSFP28 / 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
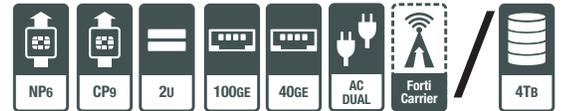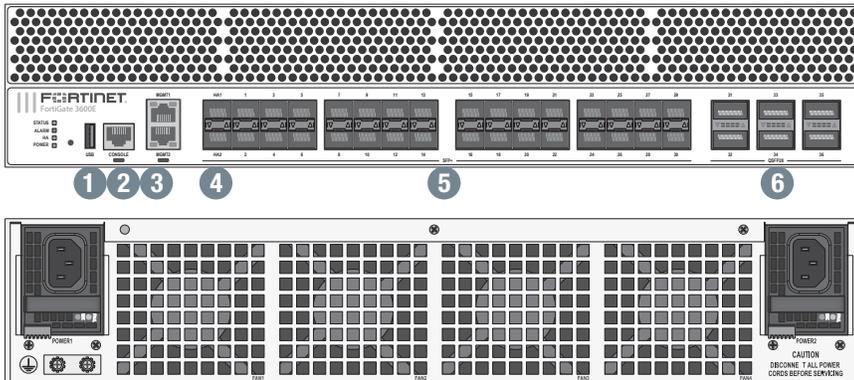
## Mobile Security for 4G, 5G, and IOT

- SPU accelerated, high performance CGNAT and IPv4 and IPv6 traffic, for 4G SGi LAN and 5G N6 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 SCTP, GTP-U/C and SIP that provides protection against attacks

- 4G and 5G cores IoT signaling storm protection

- High-speed interfaces to enable deployment flexibility
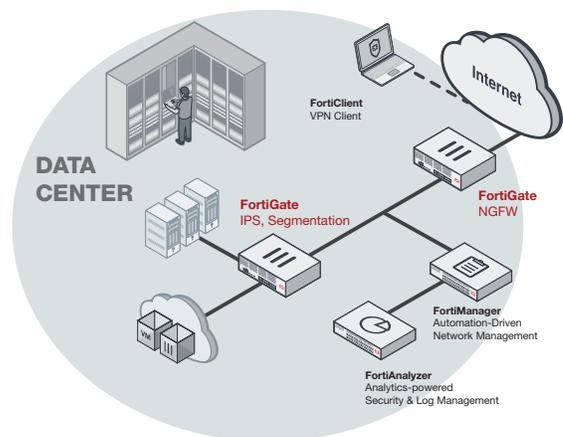


FortiGate 3600E deployment in data center
(NGFW, IPS, and Intent-based Segmentation)

F::RTINET®

# Hardware

## FortiGate 3600E/-DC and 3601E



## Interfaces

1. USB Management Port
2. Console Port
3. 2x GE RJ45 Management Ports (supports 1 GE only)
4. 2x 25 GE SFP28 / 10 GE SFP+ / GE SFP HA Slots
5. 30x 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots
6. 6x 100 GE QSFP28 / 40 GE QSFP+ 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 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 unique capability of full signature matching at SPU
- SSL Inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading

## 100 GE Connectivity for Network

High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 3600E provides multiple 100 GE QSFP28 slots, 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 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
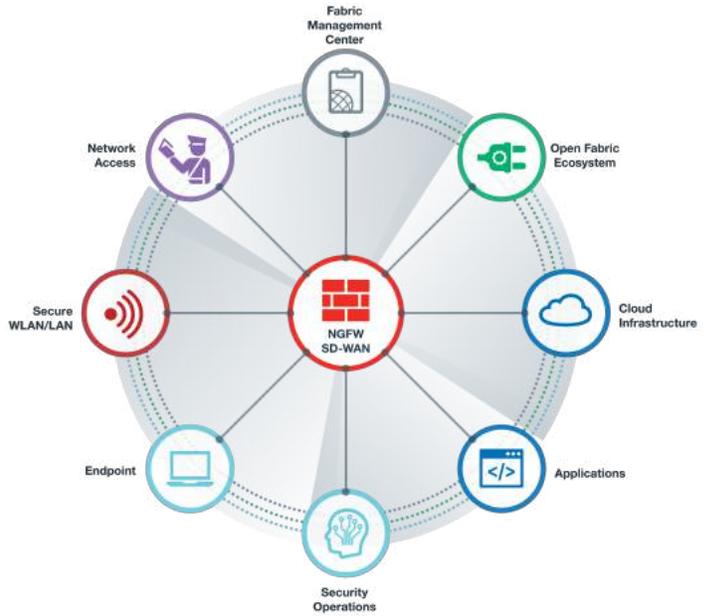
## FortiOS

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

| | FG-3600E/-DC | FG-3601E |
|---|---|---|
| **Interfaces and Modules** | | |
| 100 GE QSFP28 / 40 GE QSFP+ Slots | 6 | |
| 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots | 32 | |
| GE RJ45 Management Ports | 2 (supports 1 GE only) | |
| USB Ports (Client / Server) | 1 / 1 | |
| Console Port | 1 | |
| Internal Storage | – | 2x 2TB SSD |
| Included Transceivers | 2x SFP+ (SR 10GE) | |
| **System Performance — Enterprise Traffic Mix** | | |
| IPS Throughput [2] | 55 Gbps | |
| NGFW Throughput [2, 4] | 40 Gbps | |
| Threat Protection Throughput [2, 5] | 30 Gbps | |
| **System Performance and Capacity** | | |
| Firewall Throughput (1518 / 512 / 64 byte, UDP) | 240 / 240 / 150 Gbps | |
| IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) | 240 / 240 / 150 Gbps | |
| Firewall Latency (64 byte, UDP) | 4 µs | |
| Firewall Throughput (Packet per Second) | 225 Mpps | |
| Concurrent Sessions (TCP) | 50 Million | |
| New Sessions/Second (TCP) | 460,000 | |
| Firewall Policies | 200,000 | |
| IPsec VPN Throughput (512 byte) [1] | 145 Gbps | |
| Gateway-to-Gateway IPsec VPN Tunnels | 40,000 | |
| Client-to-Gateway IPsec VPN Tunnels | 200,000 | |
| SSL-VPN Throughput | 12 Gbps | |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | 30,000 | |
| SSL Inspection Throughput (IPS, avg. HTTPS) [3] | 34 Gbps | |
| SSL Inspection CPS (IPS, avg. HTTPS) [3] | 19,000 | |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3] | 5.2 Million | |
| Application Control Throughput (HTTP 64K) [2] | 95 Gbps | |
| CAPWAP Throughput (HTTP 64K) | 57 Gbps | |
| Virtual Domains (Default / Maximum) | 10 / 500 | |
| Maximum Number of FortiSwitches Supported | 256 | |
| Maximum Number of FortiAPs (Total / Tunnel Mode) | 4,096 / 2,048 | |
| Maximum Number of FortiTokens | 20,000 | |
| High Availability Configurations | Active / Active, Active / Passive, Clustering | |

| | FG-3600E/-DC | FG-3601E |
|---|---|---|
| **Dimensions and Power** | | |
| Height x Width x Length (inches) | 3.5 x 17.4 x 21.9 | |
| Height x Width x Length (mm) | 89 x 443 x 556 | |
| Weight | 43.1 lbs (19.6 kg) | 44.5 lbs (20.2 kg) |
| Form Factor (supports EIA / non-EIA standards) | Rack Mount, 2 RU | |
| AC Power Supply | 100–240V AC, 50–60 Hz | |
| AC Current (Maximum) | 12A@120V, 9A@240V | |
| Power Consumption (Average / Maximum) | 672 W / 977 W | |
| Heat Dissipation | 3334 BTU/h | |
| DC Power Supply (FG-3600E-DC) | -48V DC | – |
| DC Current (Maximum) | 17.8A | – |
| 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 | 60 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 3600E | FG-3600E | 6x 100 GE QSFP28 slots and 32x 25 GE SFP28 slots (including 30x ports, 2x HA ports), 2x GE RJ45 Management Ports, SPU NP6 and CP9 hardware accelerated, and 2 AC power supplies. |
| FortiGate 3600E-DC | FG-3600E-DC | 6x 100 GE QSFP28 slots and 32x 25 GE SFP28 slots (including 30x ports, 2x HA ports), 2x GE RJ45 Management Ports, SPU NP6 and CP9 hardware accelerated, and 2 DC power supplies. |
| FortiGate 3601E | FG-3601E | 6x 100 GE QSFP28 slots and 32x 25 GE SFP28 slots (including 30x ports, 2x HA ports), 2x GE RJ45 Management Ports, SPU NP6 and CP9 hardware accelerated, 4 TB SSD onboard storage, and 2 AC power supplies. |
| **Optional Accessories** | | |
| Rack Mount Sliding Rails | SP-FG3040B-RAIL | Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D/DC, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, 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-3400/3401E, FG-3600/3601E, FG-3700D, FG-3700D-NEBS, FG-3700DX, FG-3810D and FG-3815D. |
| DC power supply | SP-FG3800D-DC-PS | DC power supply for FG-3400/3401E-DC, FG-3600E-DC, FG-3700D-DC, FG-3700D-DC-NEBS, FG-3810D-DC, FG-3815D-DC. |
| 100 GE QSFP28 Transceiver Module, 4 Channel Parallel Fiber, Short Range | FG-TRAN-QSFP28-SR4 | 100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots. |
| 100 GE QSFP28 Transceiver Module, 4 Channel Parallel Fiber, Long Range | FG-TRAN-QSFP28-LR4 | 100 GE QSFP28 transceivers, 4 channel parallel fiber, long range for all systems with QSFP28 slots. |
| 40 GE QSFP+ Transceiver Module, Short Range | FG-TRAN-QSFP+SR | 40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots. |
| 40 GE QSFP+ Transceiver Module, Short Range BiDi | FG-TRAN-QSFP+SR-BIDI | 40 GE QSFP+ transceiver module, short range BiDi for all systems with QSFP+ slots. |
| 40 GE QSFP+ Transceiver Module, Long Range | FG-TRAN-QSFP+LR | 40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots. |
| 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. |
| 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. |
| 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 / 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. |
| 25 GE SFP28 Transceiver Module, Long Range | FG-TRAN-SFP28-LR | 25 GE SFP28 transceiver module, long range for all systems with SFP28 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