The FortiGate 3600E series delivers high performance threat protection and SSL inspection for large enterprises and service providers, with the flexibility to be deployed at the enterprise/cloud edge, in the data center core or internal segments. The multiple high-speed interfaces, high port density, superior security efficacy and high throughput of the 3600E series keeps your network connected and secure.

### 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 best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

### Networking
- Delivers high-performance routing capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) 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 management console that is effective, simple to use, and provides comprehensive network automation & visibility.
- Provides Zero Touch Integration with 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

### Firewalls, IPS, NGFW, Threat Protection Interfaces
- **Firewall**: 240 Gbps
- **IPS**: 55 Gbps
- **NGFW**: 40 Gbps
- **Threat Protection**: 30 Gbps
- **Interfaces**: Multiple GE RJ45, 10 GE SFP+ / GE SFP and 100 GE QSFP28 / 40 GE QSFP+ slots

Refer to specification table for details.
Deployment

Next Generation Firewall (NGFW)
- Reduce complexity by combining threat protection security capabilities into single high-performance network security appliance
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual applications in your network traffic
- Delivers industry’s highest SSL inspection performance using industry-mandated ciphers while maximizing ROI
- Proactively blocks newly discovered sophisticated attacks in real-time with advanced threat protection

Segmentation
- Intent-based Segmentation builds robust security framework while proactively reducing risk, cost and complexity
- Integrates with Security Fabric seamlessly to allow third party solutions and continuous trust assessment and thereby prevent sophisticated attacks
- Protects critical business applications and helps implement any compliance without network redesigns

Mobile Security for 4G, 5G and IOT
- SGi LAN security powered by multiple SPU’s to provide high performance CGNAT and accelerate IPv4 and IPv6 traffic
- 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
- Signaling security to inspect various protocols such as SCTP, Diameter, GTP-C, SIP and provide protection against attacks
- High-speed interfaces to enable deployment flexibility

IPS
- Highly cost-effective mitigation of unpatched vulnerability for hard-to-patch systems such as IOT, ICS, and Scada
- Protect sensitive data to achieve various regulatory compliance such as PCI, HIPPA, PII, GDPR
- Multiple inspection engines, threat intelligence feeds and advanced threat protection options to defend against unknown threats in real-time
- Best of breed intrusion prevention with high-performance SSL inspection
Hardware

FortiGate 3600E/3601E

Interfaces

1. USB Management Port
2. Console Port
3. 2x GE RJ45 Management Ports (supports 1 GE only)
4. 2x 10 GE SFP+ / GE SFP HA Slots
5. 30x 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 delivers broad visibility, integrated AI-driven breach prevention, and automated operations, orchestration, and response across all Fortinet and its ecosystem deployments. It allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between IoT, devices, and cloud environments throughout the network. All this is ties together under a single pane of glass management for significantly thereby delivering leading security capabilities across your entire environment while also significantly reducing complexity.

FortiGates are the foundation of Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet security products and Fabric-Ready Partner solutions.

FortiOS
Control all security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce complexity, costs, and response time with a truly consolidated next-generation security platform.

- A truly consolidated platform with a single OS and pane-of-glass for all security and networking services across all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance. Ability to leverage 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.
- Prevent, detect, and mitigate advanced attacks automatically in minutes with integrated AI-driven breach prevention and advanced threat protection.
- Fulfill your networking needs with extensive routing, switching, and SD-WAN capabilities along with intent-based segmentation.
- Utilize SPU hardware acceleration to boost security capability performance.

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™ 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

<table>
<thead>
<tr>
<th>Interfaces and Modules</th>
<th>FORTIGATE 3600E/3601E</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 GE QSFP28 / 40 GE QSFP+ Slots</td>
<td>6</td>
</tr>
<tr>
<td>10 GE SFP+ / 7 GE SFP Slots</td>
<td>2</td>
</tr>
<tr>
<td>GE RJ45 Management Ports</td>
<td>2 (support 1GE only)</td>
</tr>
<tr>
<td>USB Ports (Client / Server)</td>
<td>2x2</td>
</tr>
<tr>
<td>Console Port</td>
<td>1</td>
</tr>
<tr>
<td>Internal Storage</td>
<td>2x 2 TB SSD (For FG-3601E only)</td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>2x SFP+ (SR100E)</td>
</tr>
</tbody>
</table>

System Performance — Enterprise Traffic Mix

| IPS Throughput | 55 Gbps |
| NIPS Throughput | 40 Gbps |
| Threat Protection Throughput | 30 Gbps |

System Performance and Capacity

| Firewall Throughput (1518 / 512 / 64 byte, UDP) | 240 / 240 / 150 Gbps |
| Firewalls Throughput (1518 / 512 / 64 byte, UDP) | 240 / 240 / 150 Gbps |
| Firewall Latency (64 byte, UDP) | 4 µs |
| Firewall Throughput (Packet per Second) | 225 Mbps |
| Concurrent Sessions (TCP) | 50 Million |
| New Sessions/Second (TCP) | 200,000 |
| Firewall Policies | 2,000,000 |
| IPSec VPN Throughput | 15 Gbps |
| Gateway-to-Gateway IPSec VPN Tunnels | 40,000 |
| Client-to-Gateway IPSec VPN Tunnels | 20,000 |
| SSL-VPN Throughput | 12 Gbps |
| Concurrent SSL-VPN Users | 30,000 |
| (Recommended Maximum, Tunnel Mode) | |
| SSL Inspection Throughput (IPS, avg. HTTPS) | 34 Gbps |
| SSL Inspection Throughput (IPS, avg. HTTPS) | 5.2 Million |
| SSL Inspection Concurrent Session | 5.2 Million |
| Application Control Throughput (HTTP 64K) | 85 Gbps |
| Application Control Throughput (HTTP 64K) | 12 Gbps |
| Virtual Domains (Default / Maximum) | 30 / 500 |
| Maximum Number of FortiSwitches Supported | 256 |
| Maximum Number of FortiTokens | 20,000 |
| Maximum Number of Registered FortiClients | 50,000 |
| High Availability Configurations | |

Dimensions and Power

<table>
<thead>
<tr>
<th>FORTIGATE 3600E/3601E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height x Width x Length (inches)</td>
</tr>
<tr>
<td>Height x Width x Length (mm)</td>
</tr>
<tr>
<td>Weight</td>
</tr>
<tr>
<td>3601E: 44.5 lbs (20.2 kg)</td>
</tr>
<tr>
<td>Power Consumption (Average / Maximum)</td>
</tr>
</tbody>
</table>

Note: All performance values are “up to” and vary depending on system configuration.

1. IPSec VPN performance test uses AES256-SHA1-256.
2. IPS (Enterprise Mix), Application Control, NIPS and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance uses an average of HTTPS sessions of different cipher suites.
4. NIPS 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 10 GE SFP+ slots (including 30x ports, 2x HA ports), 2x GE RJ45 Management Ports, SPU NP6 and CP9 hardware accelerated, and 2 AC power supplies.

FortiGate 3601E | FG-3601E | 6x 100 GE QSFP28 slots and 32x 10 GE SFP+ 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-3300D/-DC, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC and FG-3815D

AC power supply | SP-FG3300D-P5 | AC power supply for FG-3400/3401E, FG-3600/3601E, FG-3700D, FG-3700D-NEBS, FG-3700DX, FG-3810D and FG-3815D

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-RJ45 | 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, 10 m / 32.8 ft | SP-CABLE-ADASFP+ | 10 GE SFP+ active direct attach cable, 10 m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.

Bundles

FortiGuard Bundles

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.

<table>
<thead>
<tr>
<th>Bundles</th>
<th>360 Protection</th>
<th>Enterprise Protection</th>
<th>UTM Protection</th>
<th>Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</td>
<td>ASE 1</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
<tr>
<td>FortiGuard Advanced Malware Protection (AMP) — Anti-Malware, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Web Filtering Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Web Security Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Industrial Security Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiManager Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. 24/7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.2

FortiGuard Web Filtering Service

FortiGuard Web Filtering Service provides comprehensive Web filtering capabilities to protect your network from malicious websites and phishing attacks. FortiGuard Web Filtering Service allows you to control access to websites and prevent the spread of malware.

FortiGuard Security Rating Service

FortiGuard Security Rating Service provides real-time security ratings for websites and applications. FortiGuard Security Rating Service helps you identify and block malicious websites and applications that pose a security risk to your network.

FortiGuard Industrial Security Service

FortiGuard Industrial Security Service provides comprehensive security solutions for industrial networks. FortiGuard Industrial Security Service includes features such as industrial-grade intrusion prevention, threat detection, and advanced malware protection.

FortiManager Cloud

FortiManager Cloud is a cloud-based management platform for Fortinet solutions. FortiManager Cloud allows you to centrally manage and monitor your FortiGate and other Fortinet devices from a single interface.

Protection

Enterprise Protection

UTM Protection

Threat Protection

FortiCare

ASE 1

24x7

24x7

24x7

1. 24/7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.2