The FortiGate 2600F 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 and hyperscale 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

<table>
<thead>
<tr>
<th>Firewall</th>
<th>IPS</th>
<th>NGFW</th>
<th>Threat Protection</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>198 Gbps</td>
<td>24 Gbps</td>
<td>19 Gbps</td>
<td>17 Gbps</td>
<td>Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP and 100GE QSFP28 / 40 GE QSFP+ slots</td>
</tr>
</tbody>
</table>

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

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

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

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
Hardware

FortiGate 2600F Series

Interfaces

1. 2 x GE RJ45 MGMT Ports
2. 2 x 10 GE SFP+ / GE SFP HA Slots
3. 16 x 10GE RJ45 ports
4. 16 x 25GE SFP 28 / 10GE SFP+ / GE SFP Slots
5. 4 x 100GE QSFP28 / 40GE 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

Trusted Platform Module (TPM)

The FortiGate 2600F Series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.

Network Processor

Fortinet’s latest SPU NP7 Hyperscale architecture is a purpose-built network processor that delivers accelerated hardware performance for FortiOS:

- IPv4/IPv6, SCTP, unicast, multicast and anycast
- CAPWAP, VXLAN and GRE IP tunneling
- IPSec VPN (including Suite B)
- DDoS protection in hardware against volumetric attacks, fragment reassembly, traffic shaping and priority queuing
- Elephant Flows of up to 100Gbps

Content Processor

The SPU CP9 content processor works outside of the direct flow of traffic, providing high-speed cryptography and content inspection services including:

- Signature-based content inspection acceleration
- 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 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.
## Specifications

### Hardware Specifications

<table>
<thead>
<tr>
<th>FG-2600F</th>
<th>FG-2601F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Accelerated 10GE RJ45 Ports</td>
<td>16</td>
</tr>
<tr>
<td>Hardware Accelerated 25GE SFP28 / 10GE SFP+ / GE SFP Slots</td>
<td>16</td>
</tr>
<tr>
<td>Hardware Accelerated 100GE QSFP28 / 40GE QSFP+ Slots</td>
<td>4</td>
</tr>
<tr>
<td>GE RJ45 Management Ports</td>
<td>2</td>
</tr>
<tr>
<td>2x 10GE SFP+ / GE SFP HA Slots</td>
<td>2</td>
</tr>
<tr>
<td>USB 3.0 Port</td>
<td>1</td>
</tr>
<tr>
<td>Console RJ45 Port</td>
<td>1</td>
</tr>
<tr>
<td>Onboard Storage</td>
<td>2x 1TB NVMe SSD</td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>2x SFP+ (SR 10GE)</td>
</tr>
</tbody>
</table>

### System Performance — Enterprise Traffic Mix

<table>
<thead>
<tr>
<th>FG-2600F</th>
<th>FG-2601F</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Throughput (512 byte)</td>
<td>24 Gbps</td>
</tr>
<tr>
<td>NGFW Throughput</td>
<td>19 Gbps</td>
</tr>
<tr>
<td>Threat Protection Throughput</td>
<td>17 Gbps</td>
</tr>
</tbody>
</table>

### System Performance and Capacity

<table>
<thead>
<tr>
<th>FG-2600F</th>
<th>FG-2601F</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)</td>
<td>108 / 196 / 120 Gbps</td>
</tr>
<tr>
<td>IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)</td>
<td>19 Gbps</td>
</tr>
<tr>
<td>Firewall Throughput (Packet per Second)</td>
<td>24 Million</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>1 Million</td>
</tr>
<tr>
<td>IPsec VPN Throughput (512 byte)</td>
<td>1 Million</td>
</tr>
<tr>
<td>Gateway-to-Gateway IPsec VPN Tunnels</td>
<td>20,000</td>
</tr>
<tr>
<td>Client-to-Gateway IPsec VPN Tunnels</td>
<td>100,000s</td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td>16 Gbps</td>
</tr>
<tr>
<td>Concurrent SSL-VPN Users</td>
<td>30,000</td>
</tr>
<tr>
<td>SSL Inspection Throughput (IPS, avg. HTTPS)</td>
<td>20 Gbps</td>
</tr>
<tr>
<td>SSL Inspection Throughput (IPS, avg. HTTP)</td>
<td>16 Gbps</td>
</tr>
<tr>
<td>SSL Inspection Throughput (IPS, avg. HTTPS)</td>
<td>16 Gbps</td>
</tr>
<tr>
<td>Application Control Throughput</td>
<td>64 Gbps</td>
</tr>
<tr>
<td>CAPNAP Throughput (HTTP 64K)</td>
<td>10.5 Gbps</td>
</tr>
<tr>
<td>Virtual Domains (Default / Maximum)</td>
<td>10 / 500</td>
</tr>
<tr>
<td>Maximum Number of FortiSwitches Supported</td>
<td>196</td>
</tr>
<tr>
<td>Maximum Number of FortiAPs (Total / Tunnel)</td>
<td>4,096 / 2,048</td>
</tr>
<tr>
<td>Maximum Number of FortiTokens</td>
<td>20,000</td>
</tr>
<tr>
<td>High Availability Configurations</td>
<td>Active-Active, Active-Passive, Clustering</td>
</tr>
</tbody>
</table>

### Dimensions and Power

<table>
<thead>
<tr>
<th>FG-2600F</th>
<th>FG-2601F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height x Width x Length (inches)</td>
<td>3.5 x 17.25 x 21.1</td>
</tr>
<tr>
<td>Height x Width x Length (mm)</td>
<td>88.4 x 438 x 536</td>
</tr>
<tr>
<td>Weight</td>
<td>30.6 lbs (13.9 kg)</td>
</tr>
<tr>
<td>Maximum Current</td>
<td>6A</td>
</tr>
<tr>
<td>Maximum Power Consumption</td>
<td>510 W</td>
</tr>
<tr>
<td>Average Power Consumption</td>
<td>416 W</td>
</tr>
<tr>
<td>Redundant Power Supplies</td>
<td>Yes, Hot swappable</td>
</tr>
</tbody>
</table>

### Operating Environment and Certifications

<table>
<thead>
<tr>
<th>FG-2600F</th>
<th>FG-2601F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Control, NGFW, and Threat Protection are measured with Logging enabled.</td>
<td></td>
</tr>
</tbody>
</table>

---

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

1. IPsec VPN performance test uses AES-256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW, and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance uses 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

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 2600F</td>
<td>FG-2600F</td>
<td>4 x 100GE/40GE QSFP28 slots, 16 x 25GE/10GE SFP28 slots, 16 x 10GE RJ45 ports, 2x 10G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies</td>
</tr>
<tr>
<td>FortiGate 2601F</td>
<td>FG-2601T</td>
<td>4 x 100GE/40GE QSFP28 slots, 16 x 25GE/10GE SFP28 slots, 16 x 10GE RJ45 ports, 2x 10G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with 2TB onboard storage</td>
</tr>
</tbody>
</table>

Optional Accessories

1 GE SFP+ transceiver module | PN-TRAN-LX | 1 GE SFP+ LX transceiver module for all systems with SFP and SFP/SFP+ slots. |
10 GE SFP+ transceiver module | PN-TRAN-SFP+ | 10 GE SFP+ transceiver module for all systems with SFP+ slots. |
40 GE QSFP+ transceiver module, long range | PN-TRAN-QSFP+ | 40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots. |
40 GE QSFP+ transceiver module, extended range | PN-TRAN-QSFP+ | 40 GE QSFP+ transceiver module, extended range for all systems with QSFP+ slots. |
10 GE SFP+ transceiver module, short range, BiDi | PN-TRAN-SFP+ | 10 GE SFP+ transceiver module, short range BiDi for systems with SFP+ slots. |
40 GE QSFP+ transceiver module, Long Range | PN-TRAN-QSFP+ | 40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots. |
40 GE QSFP+ transceiver module, Short Range | PN-TRAN-QSFP+ | 40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots. |
100 GE QSFP28 Transceivers | PN-TRAN-QSFP28R | 100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots. |
100 GE QSFP28 Transceivers, Short Range | PN-TRAN-QSFP28R | 100 GE QSFP28 transceivers, short range for all systems with QSFP28 slots. |
100 GE QSFP28 Transceivers, CWDM4 | PN-TRAN-QSFP28-CWDM4 | 100 GE QSFP28 transceivers, CWDM4 connectors, 24M for all systems with QSFP28 slots. |

AC power supply

Rack mounting sliding rails


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.