The FortiGate 6000F 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 network integration to the new security generation.

**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 advanced networking 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 a management console that is effective, simple to use, and provides comprehensive network automation and 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

### FEATURE

<table>
<thead>
<tr>
<th>Feature</th>
<th>FG-6300F/DC / 6301F/DC</th>
<th>FG-6500F/DC / 6501F/DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIREWALL</td>
<td>239 Gbps</td>
<td>239 Gbps</td>
</tr>
<tr>
<td>IPS</td>
<td>110 Gbps</td>
<td>170 Gbps</td>
</tr>
<tr>
<td>NGFW</td>
<td>90 Gbps</td>
<td>150 Gbps</td>
</tr>
<tr>
<td>THREAT PROTECTION</td>
<td>60 Gbps</td>
<td>100 Gbps</td>
</tr>
<tr>
<td>NETWORK INTERFACES</td>
<td>Multiple 40/100 GE QSFP28, 1/10/25 GE SFP28, 1/10 GE SFP+ and GE RJ45</td>
<td>Multiple 40/100 GE QSFP28, 1/10/25 GE SFP28, 1/10 GE SFP+ and GE RJ45</td>
</tr>
</tbody>
</table>

Refer to specification 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

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

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
HARDWARE

FortiGate 6300F/DC, 6301F/DC, 6500F/DC, 6501F/DC

Interfaces

1. Console Port
2. USB Port
3. 2x GE RJ45, 1x 1/10 GE SFP+ Management Ports
4. 2x 10 GE SFP+ HA Slots
5. 24x 1/10/25 GE SFP28 Slots
6. 4x 40/100 GE QSFP28 Slots

Hardware Features

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 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.

Distribution Processor
Fortinet's SPU DP3 distribution processor provides hardware load balancing for traffic to multiple processing units.
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 and 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.

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™ 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.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric’s ability to deliver consistent security across hybrid deployment models of Hardware, Software, and Software As-a-Service with SASE and ZTNA, among others.
SPECIFICATIONS

FORTIGATE  6300F/-DC  6301F/-DC  6500F/-DC  6501F/-DC

Interfaces and Modules

Hardware Accelerated 40/100 GE  4  
QSF28 Slots

Hardware Accelerated 1/10/25 GE  24  
SFP28 Slots

Hardware Accelerated 10 GE SFP+ Slots  3  
GE RJ45 Management Ports  2

USB Port

Console Port

Included Transceivers  2x SFP+ (SR 10 GE)

System Performance — Enterprise Traffic Mix

IPS Throughput  110 Gbps  170 Gbps

NGFW Throughput  90 Gbps  150 Gbps

Threat Protection Throughput  50 Gbps  100 Gbps

System Performance and Capacity

IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)  239 Gbps / 238 Gbps / 135 Gbps

IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)  262 Gbps / 261 Gbps / 200 Gbps

Firewall Throughput (Packet per Second)  30 Million / 20 Million

New Sessions/Second (TCP)  1 Million / 3 Million

Firewall Policies

IPSec VPN Throughput (512 byte)  96 Gbps / 100 Gbps

Gateway-to-Gateway IPSec VPN Tunnels  20,000 / 20,000

Client-to-Gateway IPSec VPN Tunnels  90,000 / 90,000

SSL-VPN Throughput  9 Gbps / 9 Gbps

Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)  30,000 / 30,000

SSL Inspection Throughput (IPS, avg. HTTPS)  66 Gbps / 110 Gbps

SSL Inspection CPS (IPS, avg. HTTPS)  10 Million / 1 Million

SSL Inspection Concurrent Session (IPS, avg. HTTPS)  15 Gbps / 20 Gbps

Application Control Throughput (HTTP 64K)  150 Gbps / 200 Gbps

CAPWAP Throughput (HTTP 64K)  N/A / N/A

Virtual Domains (Default / Maximum)  10 / 500

Maximum Number of FortiSwitches  200

Supported

Maximum Number of FortiAPs (Total / Tunnel)

Maximum Number of FortiTokens

Maximum Number of Registered FortiClients

High Availability Configurations

Dimensions and Power

Height x Width x Length (inches)  5.20 x 17.20 x 26.18  5.3 x 17.2 x 27.3

Height x Width x Length (mm)  132 x 437 x 665  133 x 437 x 694

Weight  67.68 lbs / 30.7 kg  69.00 lbs / 31.3 kg

Power Consumption

(Average / Maximum)  977 W / 1,237 W  1,328 W / 1,568 W

AC Power Supply  30W, 100–240V, 50–60 Hz

DC Current (Maximum)  4.6 – 48 VDC

Heat Dissipation  4,153 BTU/h / 4,221 BTU/h

Redundant Power Supplies  2+1 Redundant / 1+1 Redundant if using high line power

Form Factor

Rack Mount, 3 RU

AC Power Supplies

100–240V AC, 50–60 Hz

Power Consumption (Average / Maximum)

977 W / 1,237 W  1,328 W / 1,568 W

Form Factor

Rack Mount, 3 RU

AC Power Supplies

100–240V AC, 50–60 Hz

Power Consumption (Average / Maximum)

977 W / 1,237 W  1,328 W / 1,568 W

Certifications

SSL-VPN, USGv6, IPv6

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  57.43 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

ICSA Labs: Firewall, 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.
## ORDERING INFORMATION

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 6300F</td>
<td>FG-6300F</td>
<td>4x 40/100 GE QSFP28 slots, 24x 1/10/25 GE SFP28 slots, 2x 1 GE RJ45 management ports, 2x 10 GE SFP+ HA ports, 1x 1/10 GE SFP+ management port, and 3x AC power supplies.</td>
</tr>
<tr>
<td>FortiGate 6301F</td>
<td>FG-6301F</td>
<td>4x 40/100 GE QSFP28 slots, 24x 1/10/25 GE SFP28 slots, 2x 1 GE RJ45 management ports, 2x 10 GE SFP+ HA ports, 1x 1/10 GE SFP+ management port, and 3x AC power supplies.</td>
</tr>
<tr>
<td>FortiGate 6301F-DC</td>
<td>FG-6301F-DC</td>
<td>4x 40/100 GE QSFP28 slots, 24x 1/10/25 GE SFP28 slots, 2x 1 GE RJ45 management ports, 2x 10 GE SFP+ HA ports, 1x 1/10 GE SFP+ management port, and 3x AC power supplies.</td>
</tr>
<tr>
<td>FortiGate 6500F</td>
<td>FG-6500F</td>
<td>4x 40/100 GE QSFP28 slots, 24x 1/10/25 GE SFP28 slots, 2x 1 GE RJ45 management ports, and 3x AC power supplies.</td>
</tr>
<tr>
<td>FortiGate 6500F-DC</td>
<td>FG-6500F-DC</td>
<td>4x 40/100 GE QSFP28 slots, 24x 1/10/25 GE SFP28 slots, 2x 1 GE RJ45 management ports, and 3x AC power supplies.</td>
</tr>
<tr>
<td>FortiGate 6501F</td>
<td>FG-6501F</td>
<td>4x 40/100 GE QSFP28 slots, 24x 1/10/25 GE SFP28 slots, 2x 1 GE RJ45 management ports, 2x 1 TB NVMe, and 3x AC power supplies.</td>
</tr>
<tr>
<td>FortiGate 6501F-DC</td>
<td>FG-6501F-DC</td>
<td>4x 40/100 GE QSFP28 slots, 24x 1/10/25 GE SFP28 slots, 2x 1 GE RJ45 management ports, 2x 1 TB NVMe, and 3x AC power supplies.</td>
</tr>
</tbody>
</table>

### Optional Accessories/Spares

<table>
<thead>
<tr>
<th>Description</th>
<th>SKU</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 GE QSFP28 Transceiver Module, 4 Channel Parallel Fiber, Short Range</td>
<td>FG-TRAN-QSFP28-SR4</td>
</tr>
<tr>
<td>100 GE QSFP28 Transceiver Module, 4 Channel Parallel Fiber, Long Range</td>
<td>FG-TRAN-QSFP28-LR4</td>
</tr>
<tr>
<td>40 GE QSFP+ Transceiver Module, Short Range</td>
<td>FG-TRAN-QSFP+SR</td>
</tr>
<tr>
<td>40 GE QSFP+ Transceiver Module, Short Range BiDi</td>
<td>FG-TRAN-QSFP+SR-BIDI</td>
</tr>
<tr>
<td>40 GE QSFP+ Transceiver Module, Long Range</td>
<td>FG-TRAN-QSFP+LR</td>
</tr>
<tr>
<td>10 GE/25 GE SFP28 Transceiver Module, Short Range</td>
<td>FG-TRAN-SFP28-SR</td>
</tr>
<tr>
<td>25 GE SFP28 Transceiver Module, Long Range</td>
<td>FG-TRAN-SFP28-LR</td>
</tr>
<tr>
<td>10 GE SFP+ Transceiver Module, Short Range</td>
<td>FG-TRAN-SFP+SR</td>
</tr>
<tr>
<td>10 GE SFP+ Transceiver Module, Long Range</td>
<td>FG-TRAN-SFP+LR</td>
</tr>
<tr>
<td>1 GE SFP SX Transceiver Module</td>
<td>FG-TRAN-SX</td>
</tr>
<tr>
<td>10GBase-ER SFP+ Transceiver Module</td>
<td>FS-TRAN-SFP+ER</td>
</tr>
<tr>
<td>AC Power Supply</td>
<td>FG-7040E-PS-AC</td>
</tr>
</tbody>
</table>

# 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>Unified Threat Protection</th>
<th>Advanced Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</td>
<td>ASE ¹</td>
<td>24×7</td>
<td>24×7</td>
<td>24×7</td>
</tr>
<tr>
<td>FortiGuard App Control Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IPS Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Advanced Malware Protection (AMP) — Antivirus, 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 and Video Filtering Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Antispam Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Security Rating Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IoT Detection Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Industrial Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiConverter Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Orchestrator Entitlement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Cloud Assisted Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Overlay Controller VPN Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fortinet SOCaaS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiAnalyzer Cloud</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 7.0

---

1. 24×7 plus Advanced Services Ticket Handling  
2. Available when running FortiOS 7.0