The FortiGate 1800F 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 1800F series keep 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 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

<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>13 Gbps</td>
<td>11 Gbps</td>
<td>9.1 Gbps</td>
<td>Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP and 40 GE QSFP+ slots</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 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

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
HARDWARE

FortiGate 1800F Series

Interfaces

1. 2 x GE RJ45 MGMT Ports
2. 2 x 10 GE SFP+ / GE SFP HA Slots
3. 16 x GE RJ45 Ports
4. 8 x GE SFP Slots
5. 12 x 25 SFP28 / 10 GE SFP+ / GE SFP Slots
6. 4 x 40 GE QSFP+ Slots

Hardware Features

Hyperscale Firewall License
Empower organizations by unlocking further performance boosts with this perpetual license. The Hyperscale Firewall License will enable the hardware acceleration of CGNAT features by utilizing the latest SPU NP7. These features include hardware session setup, firewall session logging, and NAT.

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 NP7 network processor works inline with FortiOS functions delivering:
- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency
- VPN, CAPWAP 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.
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.

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.

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.
## SPECIFICATIONS

<table>
<thead>
<tr>
<th>Interfaces and Modules</th>
<th>FG-1800F/-DC</th>
<th>FG-1801F/-DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Accelerated GE RJ45 Ports</td>
<td>16</td>
<td>12</td>
</tr>
<tr>
<td>Hardware Accelerated GE SFP Slots</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Hardware Accelerated 40GE QSFP+ Slots</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td>GE RJ45 Management Ports</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10 GE SFP+ / GE SFP HA Slots</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>USB 3.0 Port</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Console RJ45 Port</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Onboard Storage</td>
<td>0</td>
<td>2x 1 TB NVMe SSD</td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>2x SFP+ (SR 10GE)</td>
<td></td>
</tr>
</tbody>
</table>

### System Performance — Enterprise Traffic Mix

- **IPS Throughput**
  - FG-1800F/-DC: 13 Gbps
  - FG-1801F/-DC: 11 Gbps

- **NGFW Throughput**
  - FG-1800F/-DC: 11 Gbps
  - FG-1801F/-DC: 9.1 Gbps

- **Threat Protection Throughput**
  - FG-1800F/-DC: 9.1 Gbps
  - FG-1801F/-DC: 8 Gbps

### System Performance and Capacity

- **IPv4 Firewall Throughput**
  - (1518 / 512 / 64 byte, UDP)
  - FG-1800F/-DC: 198 / 197 / 140 Gbps
  - FG-1801F/-DC: 198 / 197 / 140 Gbps

- **IPv6 Firewall Throughput**
  - (1518 / 512 / 64 byte, UDP)
  - FG-1800F/-DC: 3.22 μs
  - FG-1801F/-DC: 12 Million / 40 Million

- **Firewall Latency (64 byte, UDP)**
  - FG-1800F/-DC: 210 Mpps
  - FG-1801F/-DC: 210 Mpps

- **New Sessions/Second (TCP)**
  - FG-1800F/-DC: 750,000 / 2 Million
  - FG-1801F/-DC: 750,000 / 2 Million

- **Firewall Policies**
  - FG-1800F/-DC: 100,000
  - FG-1801F/-DC: 100,000

- **IPsec VPN Throughput (512 byte)**
  - FG-1800F/-DC: 55 Gbps
  - FG-1801F/-DC: 55 Gbps

- **Gateway-to-Gateway IPsec VPN Tunnels**
  - FG-1800F/-DC: 20,000
  - FG-1801F/-DC: 20,000

- **Client-to-Gateway IPsec VPN Tunnels**
  - FG-1800F/-DC: 100,000
  - FG-1801F/-DC: 100,000

- **SSL-VPN Throughput**
  - FG-1800F/-DC: 11 Gbps
  - FG-1801F/-DC: 11 Gbps

- **Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)**
  - FG-1800F/-DC: 10,000
  - FG-1801F/-DC: 10,000

- **SSL Inspection Throughput (IPS, avg. HTTPS)**
  - FG-1800F/-DC: 17 Gbps
  - FG-1801F/-DC: 17 Gbps

- **SSL Inspection Concurrent Session (IPS, avg. HTTPS)**
  - FG-1800F/-DC: 9.500
  - FG-1801F/-DC: 9.500

- **SSL Inspection CPS (IPS, avg. HTTPS)**
  - FG-1800F/-DC: 1.3 Million
  - FG-1801F/-DC: 1.3 Million

- **Application Control Throughput (HTTP 64K)**
  - FG-1800F/-DC: 34 Gbps
  - FG-1801F/-DC: 34 Gbps

- **CAPWAP Throughput (HTTP 64K)**
  - FG-1800F/-DC: 95 Gbps
  - FG-1801F/-DC: 95 Gbps

- **Virtual Domains (Default / Maximum)**
  - FG-1800F/-DC: 10 / 250
  - FG-1801F/-DC: 10 / 250

### Maximum Number of FortiSwitches Supported

- FG-1800F/-DC: 196

### Maximum Number of FortiAPs

- (Total / Tunnel)
  - FG-1800F/-DC: 4,096 / 2,048
  - FG-1801F/-DC: 4,096 / 2,048

### Maximum Number of FortiTokens

- FG-1800F/-DC: 20,000

### Maximum Number of Registered FortiClients

- FG-1800F/-DC: --

### High Availability Configurations

- Active-Active, Active-Passive, Clustering

---

**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.

---

**Dimensions and Power**

<table>
<thead>
<tr>
<th>FG-1800F/-DC</th>
<th>FG-1801F/-DC</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 538</td>
</tr>
<tr>
<td>Weight</td>
<td>30.2 lbs (13.7 kg) / 30.4 lbs (13.8 kg)</td>
</tr>
</tbody>
</table>

**Form Factor**

- Rack Mount, 2RU

**AC Power Supply**

- 100–240VAC, 50/60 Hz

**AC Current (Maximum)**

- 7A@100VAC, 3A@240VAC

**DC Power Supply**

- Up to 7,400 ft (2,250 m)

**DC Current (Maximum)**

- 20A

**Power Consumption**

- Average / Maximum
  - FG-1800F/-DC: 388.3 W / 543.6 W
  - FG-1801F/-DC: 398.1 W / 558.8 W

**Heat Dissipation**

- 1,854.84 BTU/h / 1,906.70 BTU/h

**High Availability Configurations**

- Active-Active, Active-Passive, Clustering

---

**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 1800F</td>
<td>FG-1800F</td>
<td>4 x 40GE QSFP+ slots, 12 x 25GE SFP28 /10GE SFP+ slots, 2x10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports, SPU NP7 and CP9 hardware accelerated.</td>
</tr>
<tr>
<td>FortiGate 1801F</td>
<td>FG-1801F</td>
<td>4 x 40GE QSFP+ slots, 12 x 25GE SFP28 /10GE SFP+ slots, 2x10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports, SPU NP7 and CP9 hardware accelerated, 2x 1TB on board SSD storage.</td>
</tr>
<tr>
<td>FortiGate 1800F-DC</td>
<td>FG-1800F-DC</td>
<td>4 x 40GE QSFP+ slots, 12 x 25GE SFP28 /10GE SFP+ slots, 2x10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports, SPU NP7 and CP9 accelerated, dual DC power supplies.</td>
</tr>
<tr>
<td>FortiGate 1801F-DC</td>
<td>FG-1801F-DC</td>
<td>4 x 40GE QSFP+ slots, 12 x 25GE SFP28 /10GE SFP+ slots, 2x10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports, 2x1TB on board SSD storage. SPU NP7 and CP9 accelerated, dual DC power supplies.</td>
</tr>
<tr>
<td>Hyperscale Firewall License FG1KF2KF</td>
<td>LIC-FGT-HYPSC-1K2K</td>
<td>Hyperscale Firewall License for FortiGate FG1800F/FG1801F/FG2600F/FG2601F Series for hardware acceleration</td>
</tr>
</tbody>
</table>

## Optional Accessories

<table>
<thead>
<tr>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FN-TRAN-LX</td>
<td>1GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>FN-TRAN-GC</td>
<td>1GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>FN-TRAN-SX</td>
<td>1GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>SP-CABLE-ADASFP+</td>
<td>10GE SFP+ active direct attach cable, 10m /32.8 ft for all systems with SFP+ and SFP+ slots.</td>
</tr>
<tr>
<td>SP-TRAN-SFPP+SR</td>
<td>10GE SFP+ transceiver module, short range for all systems with SFP+ and SFP+ slots.</td>
</tr>
<tr>
<td>SP-TRAN-SFPP+LS</td>
<td>10GE SFP+ transceiver module, long range for all systems with SFP+ and SFP+ slots.</td>
</tr>
<tr>
<td>SP-CABLE-ADASFP+</td>
<td>10GE SFP+ active direct attach cable, 10m /32.8 ft for all systems with SFP+ and SFP+ slots.</td>
</tr>
<tr>
<td>SP-TRAN-SFPP+SRBIDI</td>
<td>40GE QSFP+ transceivers, short range BIDI for systems with QSFP+ slots.</td>
</tr>
<tr>
<td>SP-TRAN-SFPP+SR</td>
<td>40GE QSFP+ transceivers, short range for all systems with QSFP+ slots.</td>
</tr>
<tr>
<td>SP-TRAN-SFPP+LR</td>
<td>40GE QSFP+ transceivers, long range for all systems with QSFP+ slots.</td>
</tr>
<tr>
<td>SP-CABLE-ADASFP+</td>
<td>10GE SFP+ transceiver module, extended range.</td>
</tr>
<tr>
<td>SP-CABLE-ADASFP+</td>
<td>10GE SFP+ transceiver module, extended range.</td>
</tr>
<tr>
<td>FG-TRAN-QSFP+SR</td>
<td>25GE/10GE dual rate SFP28 transceiver module, long range for all systems with SFP28/ SFP+ slots.</td>
</tr>
<tr>
<td>SP-FG1800F-PS</td>
<td>AC power supply for FG-1800/1801F.</td>
</tr>
<tr>
<td>SP-FG1800F-DC-PS</td>
<td>DC power supply for FG-1800/1801F and FG-2600/2601.</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 360 Security Rating Service</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