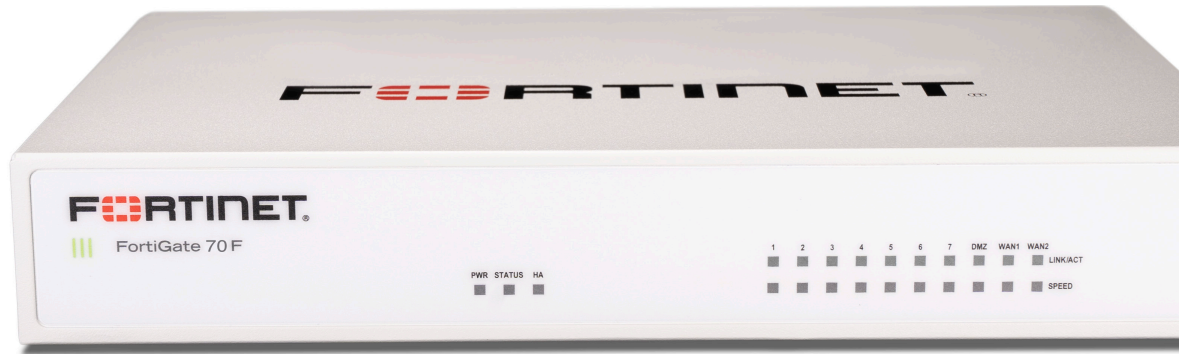


FortiGate 70F Series

FG-70F and FG-71F



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and SD-WAN.

Security-Driven Networking with FortiOS delivers converged networking and security.

Unparalleled Performance with Fortinet's patented SoC processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Simplified Operations with centralized management for networking and security, automation, deep analytics, and self-healing.

Converged Next-Generation Firewall (NGFW) and SD-WAN

The FortiGate Next-Generation Firewall 70F series is ideal for building security-driven networks at distributed enterprise sites and transforming WAN architecture at any scale.

With a rich set of AI/ML-based FortiGuard security services and our integrated Security Fabric platform, the FortiGate 70F series delivers coordinated, automated, end-to-end threat protection across all use cases.

FortiGate has the industry's first integrated SD-WAN and zero-trust network access (ZTNA) enforcement within an NGFW solution and is powered by one OS. FortiGate 70F automatically controls, verifies, and facilitates user access to applications, delivering consistency with a seamless and optimized user experience.

| IPS | NGFW | Threat Protection | Interfaces |
|----------|--------|-------------------|---|
| 1.4 Gbps | 1 Gbps | 800 Mbps | Multiple GE RJ45 Variants with internal storage |



Available in



Appliance



Virtual



Hosted



Cloud



Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

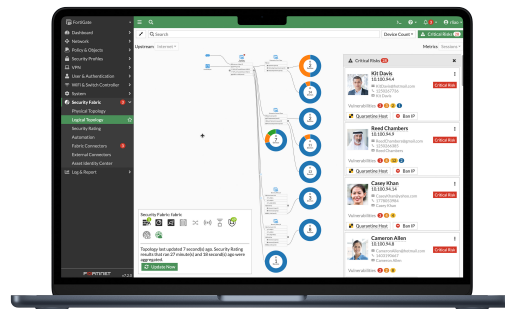
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations



Intuitive easy to use view into the network and endpoint vulnerabilities



Visibility with FOS Application Signatures

FortiConverter Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.





FortiGuard Services

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

Zero-Day Threat Prevention

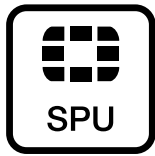
Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

OT Security

The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.



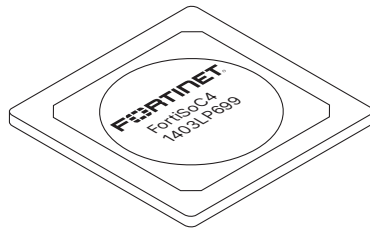
Secure Any Edge at Any Scale



Powered by Security Processing Unit (SPU)

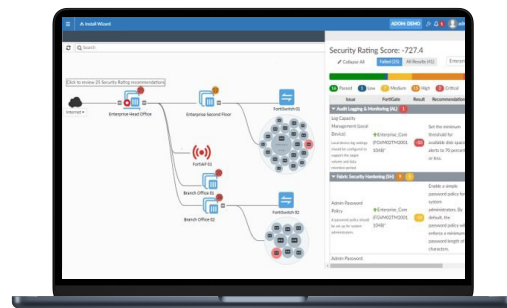
Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

ASIC Advantage



Secure SD-WAN ASIC SOC4

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience on direct internet access
- Enables best of breed NGFW Security and Deep SSL Inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity



Intuitive view and clear insights into network security posture with FortiManager

Centralized Network and Security Management at Scale

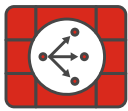
FortiManager, the centralized management solution from Fortinet, enables integrated management of the Fortinet security fabric, including devices like FortiGate, FortiSwitch, and FortiAP. It simplifies and automates the oversight of network and security functions across diverse environments, serving as the fundamental component for deploying Hybrid Mesh Firewalls.

Use Cases



Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection



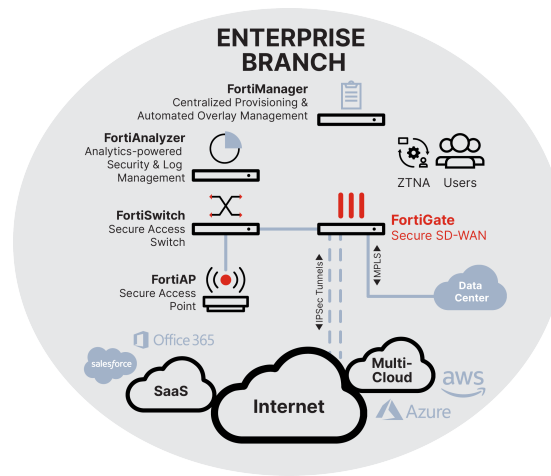
Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing



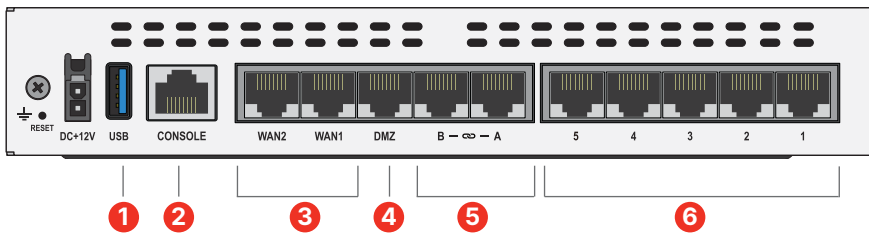
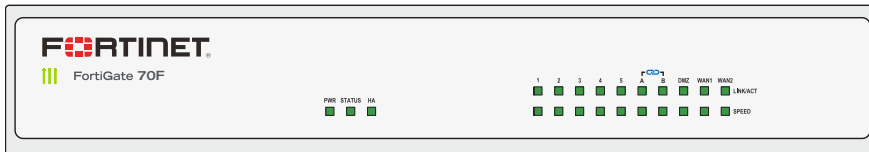
Universal ZTNA

- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access - every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD



Hardware

FortiGate 70F/71F



Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 WAN Ports
4. 1 x GE RJ45 DMZ Port
5. 2 x GE RJ45 FortiLink Ports
6. 5 x GE RJ45 Internal Ports

Hardware Features



Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight, yet highly reliable with a superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Access Layer Security

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

Specifications

| | FORTIGATE 70F | FORTIGATE 71F |
|--|---|----------------|
| Hardware Specifications | | |
| GE RJ45 WAN / DMZ Ports | 2 / 1 | 2 / 1 |
| GE RJ45 Internal Ports | 5 | 5 |
| GE RJ45 FortiLink Ports (Default) | 2 | 2 |
| Wireless Interface | – | – |
| USB Ports | 1 | 1 |
| Console (RJ45) | 1 | 1 |
| Internal Storage | – | 1 × 128 GB SSD |
| Trusted Platform Module (TPM) | No | No |
| Bluetooth Low Energy (BLE) | No | No |
| System Performance* — Enterprise Traffic Mix | | |
| IPS Throughput ² | | 1.4 Gbps |
| NGFW Throughput ^{2,4} | | 1 Gbps |
| Threat Protection Throughput ^{2,5} | | 800 Mbps |
| System Performance and Capacity | | |
| Firewall Throughput (1518 / 512 / 64 byte UDP packets) | | 10/10/6 Gbps |
| Firewall Latency (64 byte UDP packets) | | 2.54 μs |
| Firewall Throughput (Packets Per Second) | | 9 Mpps |
| Concurrent Sessions (TCP) | | 1.5 M |
| New Sessions/Second (TCP) | | 35 000 |
| Firewall Policies | | 5000 |
| IPsec VPN Throughput (512 byte) ¹ | | 6.1 Gbps |
| Gateway-to-Gateway IPsec VPN Tunnels | | 200 |
| Client-to-Gateway IPsec VPN Tunnels | | 500 |
| SSL-VPN Throughput ⁶ | | 405 Mbps |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | | 200 |
| SSL Inspection Throughput (IPS, avg. HTTPS) ³ | | 700 Mbps |
| SSL Inspection CPS (IPS, avg. HTTPS) ³ | | 500 |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³ | | 100 000 |
| Application Control Throughput (HTTP 64K) ² | | 1.8 Gbps |
| CAPWAP Throughput (HTTP 64K) | | 8.5 Gbps |
| Virtual Domains (Default / Maximum) | | 10 / 10 |
| Maximum Number of FortiSwitches Supported | | 24 |
| Maximum Number of FortiAPs (Total / Tunnel Mode) | | 64 / 32 |
| Maximum Number of FortiTokens | | 500 |
| High Availability Configurations | Active-Active, Active-Passive, Clustering | |

| | FORTIGATE 70F | FORTIGATE 71F |
|---|---|-----------------|
| Dimensions | | |
| Height x Width x Length (inches) | 1.5 × 8.5 × 6.3 | |
| Height x Width x Length (mm) | 38.5 × 216 × 160 mm | |
| Weight | 2.23 lbs (1.01 kg) | |
| Form Factor | Desktop | |
| Operating Environment and Certifications | | |
| Power Rating | 12VDC, 3A | |
| Power Required | Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz | |
| Maximum Current | 100VAC/1.0A, 240VAC/0.6A | |
| Power Consumption (Average / Maximum) | 10.17 W / 12.43 W | 17.2 W / 18.7 W |
| Heat Dissipation | 63.1 BTU/hr | 63.8 BTU/hr |
| Operating Temperature | 32°–104°F (0°–40°C) | |
| Storage Temperature | –31°–158°F (–35°–70°C) | |
| Humidity | Humidity 10%–90% non-condensing | |
| Noise Level | Fanless 0 dBA | |
| Operating Altitude | Up to 7400 ft (2250 m) | |
| Compliance | FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB | |
| Certifications | 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.

⁶ Uses RSA-2048 certificate.



Subscriptions

| Service Category | Service Offering | A-la-carte | Bundles | | |
|-------------------------------|---|------------|-----------------------|--------------------------------------|--------------------------------------|
| | | | Enterprise Protection | Unified Threat Protection | Advanced Threat Protection |
| FortiGuard Security Services | IPS Service | • | • | • | • |
| | Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service | • | • | • | • |
| | URL, DNS & Video Filtering Service | • | • | • | |
| | Anti-Spam | | • | • | |
| | AI-based Inline Malware Prevention Service | • | • | | |
| | Data Loss Prevention Service ¹ | • | • | | |
| | OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) ¹ | • | | | |
| | Application Control | | | included with FortiCare Subscription | |
| | CASB SaaS Control | | | included with FortiCare Subscription | |
| SD-WAN and SASE Services | SD-WAN Underlay Bandwidth and Quality Monitoring Service | • | | | |
| | SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning | • | | | |
| | SD-WAN Connector for FortiSASE Secure Private Access | • | | | |
| | FortiSASE subscription including cloud management and 10Mbps bandwidth license ² | • | | | |
| NOC and SOC Services | FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) ¹ | • | • | | |
| | FortiConverter Service | • | • | | |
| | Managed FortiGate Service | • | | | |
| | FortiGate Cloud (SMB Logging + Cloud Management) | • | | | |
| | FortiManager Cloud | • | | | |
| | FortiAnalyzer Cloud | • | | | |
| | FortiAnalyzer Cloud with SOCaaS | • | | | |
| | FortiGuard SOCaaS | • | | | |
| Hardware and Software Support | FortiCare Essentials ² | • | • | • | • |
| | FortiCare Premium | • | • | • | • |
| | FortiCare Elite | • | | | |
| Base Services | Internet Service (SaaS) DB Updates | | | | |
| | GeoIP DB Updates | | | | included with FortiCare Subscription |
| | Device/OS Detection Signatures | | | | |
| | Trusted Certificate DB Updates | | | | |
| | DDNS (v4/v6) Service | | | | |

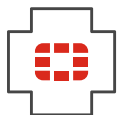
1. Full features available when running FortiOS 7.4.1

2. Desktop Models only



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.



FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive lifecycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service variants, offers heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an Extended End-of-Engineering-Support of 18 months, providing flexibility. Access the intuitive FortiCare Elite Portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.



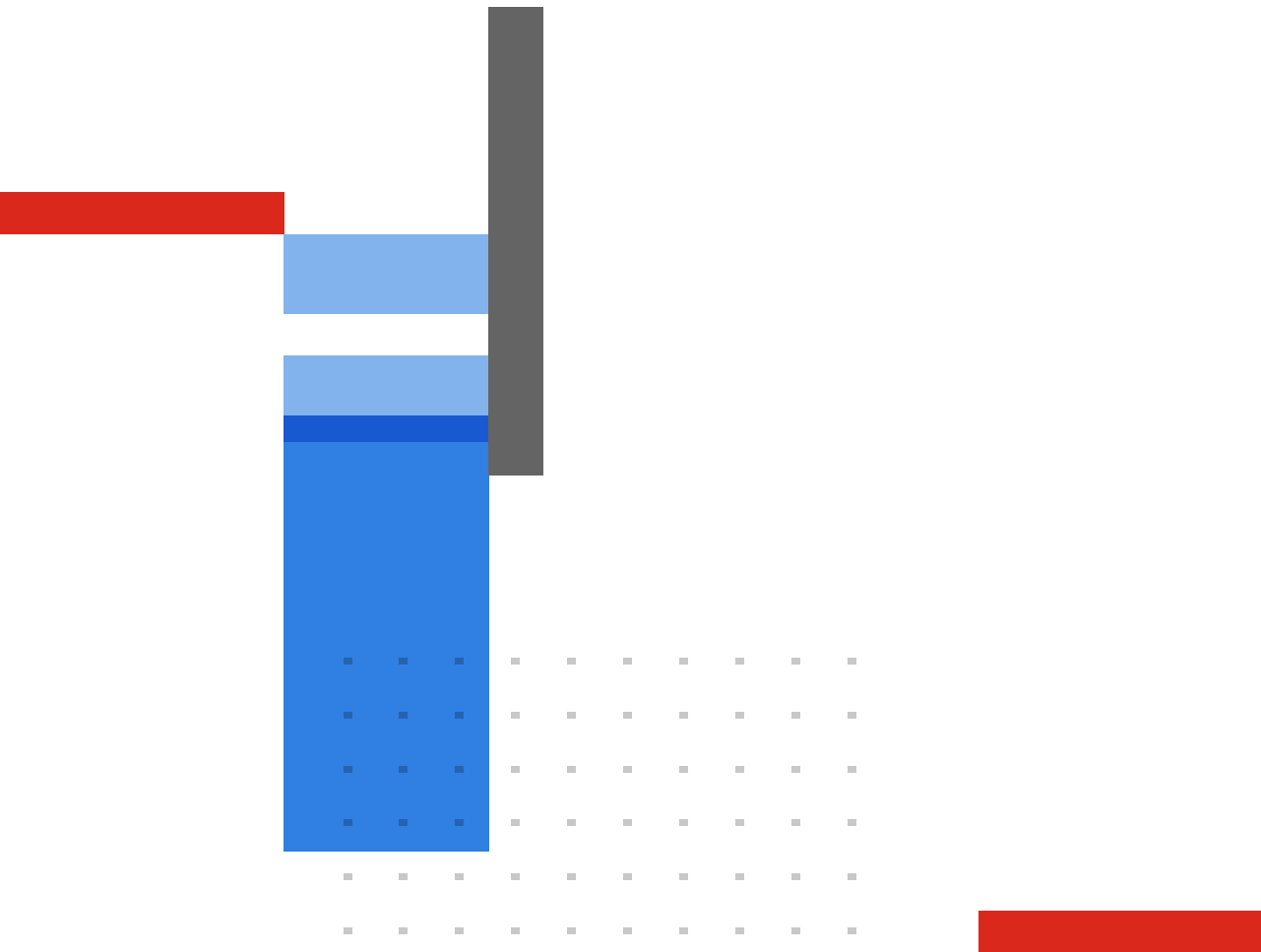
Ordering Information

| Product | SKU | Description |
|-----------------------------|-------------------|--|
| FortiGate 70F | FG-70F | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port). |
| FortiGate 71F | FG-71F | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage. |
| Optional Accessories | | |
| Rack Mount Tray | SP-RACKTRAY-02 | Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01. |
| AC Power Adaptor | SP-FG60E-PDC-5 | Pack of 5 AC power adaptors for FG/FWF 60E/61E, FG/FWF 60F/61F, FG-70F/71F, and FG-80E/81E. |
| Wall Mount Kit | SP-FG60F-MOUNT-20 | Pack of 20 wall mount kits for FG/FWF-60F, FG-70F/71F and FG/FWF-80F series. |



Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.