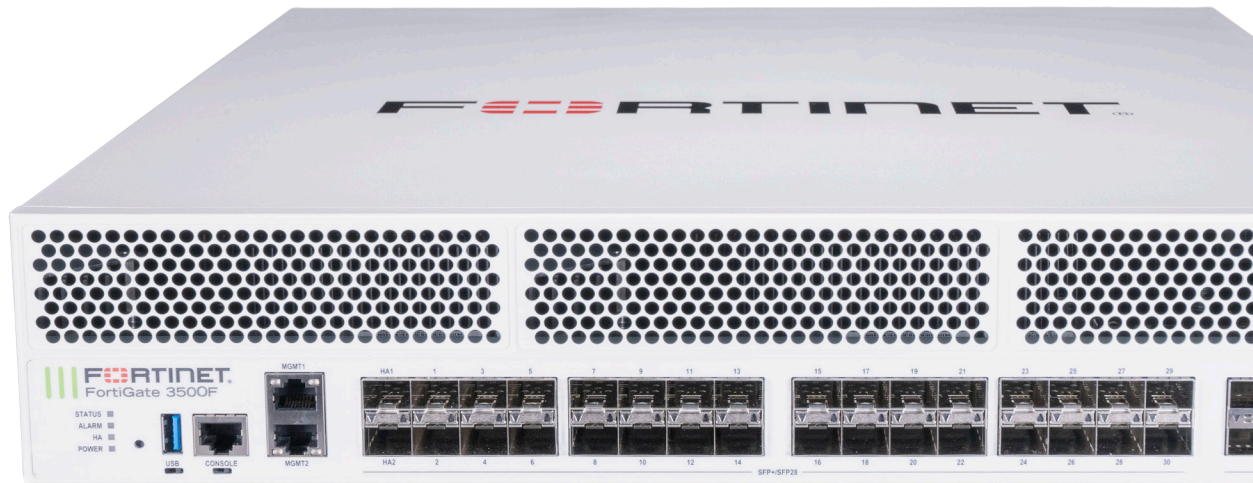


# FortiGate 3500F Series



## Highlights

**Gartner® Magic Quadrant™ Leaders** for both Network Firewalls and SD-WAN

**Secure networking** with FortiOS for converged networking and security

**Unparalleled performance** with Fortinet's patented SPU and vSPU processors

**Enterprise security** with consolidated AI / ML-powered FortiGuard services

**Hyperscale security** to secure any edge at any scale

## High Performance with Flexibility

The FortiGate 3500F series of next-generation firewalls (NGFWs) enables organizations to build secure networks that can weave security deep into their data center and across their hybrid IT architecture to protect any edge at any scale.

Powered by a rich set of AI/ML-based FortiGuard Services and an integrated Fortinet Security Fabric platform, the FortiGate 3500F series delivers coordinated, automated, end-to-end threat protection across all use cases.

The industry's first integrated zero-trust network access (ZTNA) enforcement within an NGFW solution, the FortiGate 3500F automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users for seamless user experience.

IPS	NGFW	Threat Protection	Interfaces
72 Gbps	65 Gbps	63 Gbps	Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP and 100 GE QSFP28 / 40 GE QSFP+ slots

## 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, malware, zero days, and sophisticated AI-powered 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 technology provides industry-leading high-performance protection



### Segmentation

- Dynamic segmentation adapts to any network topology to deliver true end-to-end security from the branch to the data center and across multi-cloud environments
- Ultra-scalable, low latency, VXLAN segmentation bridges physical and virtual domains with Layer 4 firewall rules
- Prevents lateral movement across the network with advanced, coordinated protection from FortiGuard Security Services, detects and prevents known, zero-day, and unknown attacks



### 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 hybrid working models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing



### Hyperscale

- Purpose-built SPUs power FortiOS to consolidate networking and security and deliver ultra-scalable secure networks.
- Unparalleled ultra-high performance offers the industry's highest number of connections and connections per second performance combined with security-enabled performance to safeguard business-critical applications.
- Hardware assisted anti-DDoS prevents volumetric attacks and delivers a strong security posture.



### Mobile Security for 4G, 5G, and IoT

- SPU-accelerated, high-performance CGNAT and IPv6 migration options, including: NAT44, NAT444, NAT64/DNS64, NAT46 for 4G Gi/sGi, and 5G N6 connectivity and security
- Radio access network security with highly scalable and highest-performing IPsec aggregation and control security gateway
- User plane security enabled by full threat protection and visibility into GTP-U inspection





## FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Infused with the latest threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero-day and sophisticated AI-powered attacks.

### Network and file security

Network and file security services protect against network and file-based threats. With over 18,000 signatures, our industry-leading intrusion prevention system (IPS) uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, and applying virtual patches for newly discovered vulnerabilities. Anti-malware protection defends against both known and unknown file-based threats, combining antivirus and sandboxing for multi-layered security. Application control improves security compliance and provides real-time visibility into applications and usage.

### Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of over 300 million URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks. FortiGuard Labs blocks over 500 million malicious/phishing/spam URLs weekly, and blocks 32,000 botnet command-and-control attempts every minute, demonstrating the robust protection offered through Fortinet.

### SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This includes data loss prevention to ensure visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. Our inline cloud access security broker service protects data in motion, at rest, and in the cloud, enforcing compliance standards and managing account, user, and cloud app usage. Services also assess infrastructure, validate configurations, and highlight risks and vulnerabilities, including IoT device detection and vulnerability correlation.

### Zero-Day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown malware in real time, delivering sub-second protection across all NGFWs. The service also integrates the MITRE ATT&CK matrix to speed up investigations. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

### OT security

With over 1000 virtual patches, 1100+ OT applications, and 3300+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.





Available in



Appliance



Virtual



Hosted



Cloud



Container

## FortiOS Everywhere

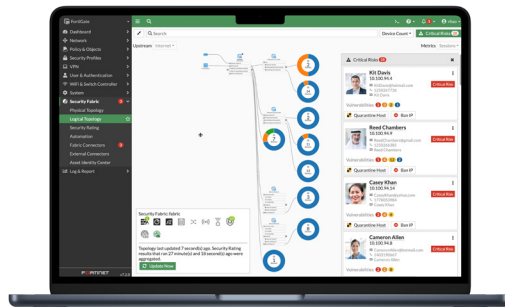
### FortiOS, Fortinet's Real-Time Network Security Operating System

FortiOS is the operating system that powers Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. FortiOS provides a unified framework for managing and securing networks, cloud-based, hybrid, or a convergence of IT, OT, and IoT. FortiOS enables seamless and efficient interoperation across Fortinet products with consistent and consolidated AI-powered protection across today's hybrid environments.

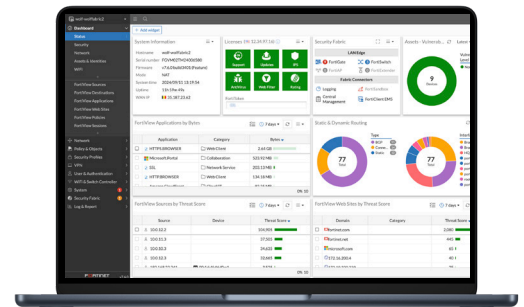
Unlike traditional point solutions, Fortinet adopts a holistic approach to cybersecurity, aiming to reduce complexities, eliminate security silos, and improve operational efficiencies. By consolidating security functions into a single platform, FortiOS simplifies management, reduces costs, and enhances overall security posture. Together, FortiGate and FortiOS create intelligent, adaptive protection to help organizations reduce complexity, eliminate security silos, and optimize user experience.

By integration generative AI (GenAI), FortiOS further enhances the ability to analyze network traffic and threat intelligence, detects deviations or anomalies more effectively, and provides more precise remediation recommendations, ensuring minimum performance impact without compromising security.

Learn more about what's new in FortiOS. <https://www.fortinet.com/products/fortigate/fortios>



*Intuitive easy to use view into the network and endpoint vulnerabilities*



*Comprehensive view of network performance, security, and system status*



## Fortinet ASICs: Unrivaled Security, Unprecedented Performance



### Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

---

### Network processor NP7

Network processors operate in line to deliver unmatched performance and scalability for critical network functions. Fortinet's breakthrough SPU NP7 works in line with FortiOS functions to deliver:

- Hyperscale firewall, accelerated session setup, and ultra-low latency
- Industry-leading performance for VPN, VXLAN termination, hardware logging, and elephant flows

---

### Content processor CP9

Content processors act as co-processors to offload resource-intensive processing of security functions. The ninth generation of the Fortinet Content Processor, the CP9, accelerates resource-intensive SSL (including TLS 1.3) decryption and security functions while delivering:

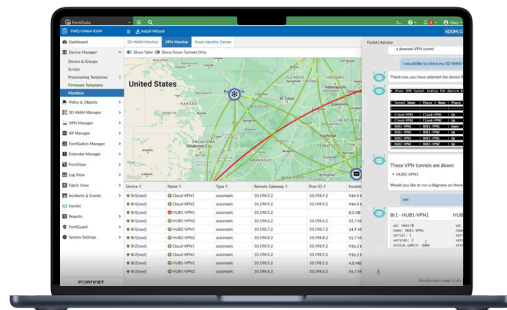
- Pattern matching acceleration and fast inspection of real-time traffic for application identification
- IPS pre-scan/pre-match, signature correlation offload, and accelerated antivirus processing

## FortiManager

### Centralized management at scale for distributed enterprises



FortiManager, powered by FortiAI, is a centralized management solution for the Fortinet Security Fabric. It streamlines mass provisioning and policy management for FortiGate, FortiGate VM, cloud security, SD-WAN, SD-Branch, FortiSASE, and ZTNA in hybrid environments. Additionally, FortiManager provides real-time monitoring of the entire managed infrastructure and automates network operation workflows. Leveraging GenAI in FortiAI, it further enhances Day 0–1 configurations and provisioning, and Day N troubleshooting and maintenance, unlocking the full potential of the Fortinet Security Fabric and significantly boosting operational efficiency.



*GenAI in FortiManager helps manage networks effortlessly—generates configuration and policy scripts, troubleshoots issues, and executes recommended actions.*

## FortiConverter Service

### Migration to FortiGate NGFW made easy



The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. 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.

## FortiCare Services

### Expertise at your service

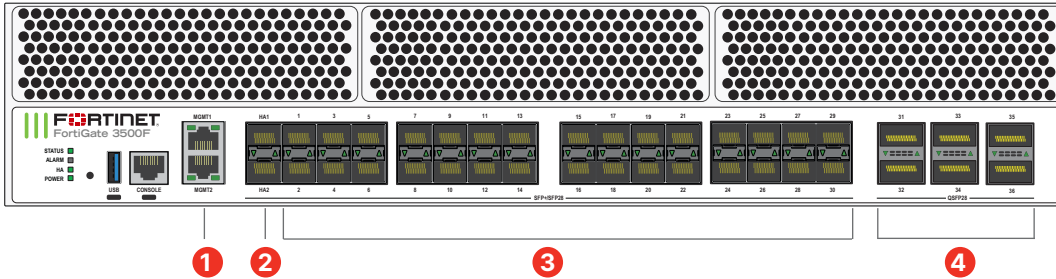


Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an extended end-of-engineering support of 18 months, providing flexibility and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.



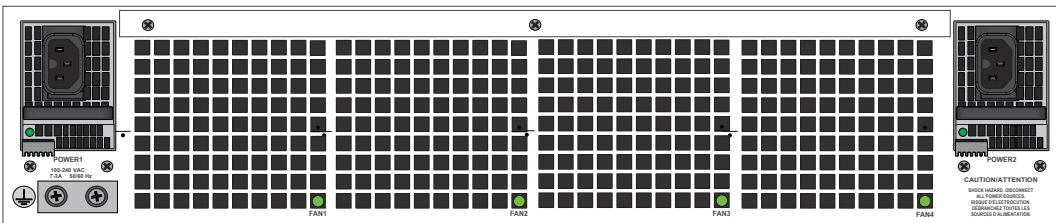
# Hardware

## FortiGate 3500F Series



### Interfaces

1. 2 × 10 GE / GE RJ45 Management Ports
2. 2 × 25 GE SFP28 / 10 GE SFP+ HA Slots
3. 30 × 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots
4. 6 × 100 GE QSFP28 / 40 GE QSFP+ Slots



### Hardware Features



### Hyperscale Firewall License



This perpetual license empowers organizations by unlocking further performance boosts. The Hyperscale Firewall License enables the hardware acceleration of CGNAT features by utilizing Fortinet’s patented SPU NP7. These features include hardware session setup, firewall session logging, and NAT.

### Trusted Platform Module (TPM)



The FortiGate 3500F 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.

## Specifications

	FG-3500F	FG-3501F
<b>Interfaces and Modules</b>		
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots		6
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots		32
10GE/ GE RJ45 Management Ports		2
USB Ports (Client / Server)		1 / 1
Console Port		1
Onboard Storage	—	2x 2TB SSD
Trusted Platform Module (TPM)		☑
Bluetooth Low Energy (BLE)		—
Signed Firmware Hardware Switch		—
Included Transceivers		2x SFP+ (SR 10 GE)
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		72 Gbps
NGFW Throughput <sup>2,4</sup>		65 Gbps
Threat Protection Throughput <sup>2,5</sup>		63 Gbps
<b>System Performance and Capacity</b>		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)		595 / 590 / 420 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)		595 / 590 / 420 Gbps
Firewall Latency (64 byte, UDP)		2.98 μs
Firewall Throughput (Packet per Second)		630 Mpps
Concurrent Sessions (TCP)		140 Million / 348 Million*
New Sessions/Second (TCP)		1 Million / 5 Million*
Firewall Policies		200 000
IPsec VPN Throughput (512 byte) <sup>1</sup>		165 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		40 000
Client-to-Gateway IPsec VPN Tunnels		200 000
SSL-VPN Throughput		16 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		30 000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>		63 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>		60 000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>		15 Million
Application Control Throughput (HTTP 64K) <sup>2</sup>		135 Gbps
CAPWAP Throughput (HTTP 64K)		65 Gbps
Virtual Domains (Default / Maximum)		10 / 500
Maximum Number of FortiSwitches Supported		300
Maximum Number of FortiAPs (Total / Tunnel)		4096 / 2048
Maximum Number of FortiTokens		20 000
High Availability Configurations		Active-Active, Active-Passive, Clustering

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

<sup>1</sup> IPsec VPN performance test uses AES256-SHA256.

<sup>2</sup> IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

<sup>3</sup> SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

	FG-3500F	FG-3501F
<b>Dimensions and Power</b>		
Height x Width x Length (inches)	3.5 × 17.4 × 21.9	
Height x Width x Length (mm)	89 × 443 × 556	
Weight	43.8 lbs (19.9 kg)	45.3 lbs (20.6 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2 RU	
AC Power Supply	100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	760 W / 1174 W	765 W / 1181 W
AC Current (Maximum)	12A@120V, 9A@240V	
Heat Dissipation	4006 BTU/h	4030 BTU/h
Redundant Power Supplies (Hot Swappable)	☑ (Default dual AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80Plus Compliant	
<b>Operating Environment and Certifications</b>		
Operating Temperature	32°F to 104°F (0°C to 40°C)	
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	
Humidity	20% to 90% non-condensing	
Noise Level	53.5 dBA	
Forced Airflow	Front to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	USGv6/IPv6	

\*Requires Hyperscale Firewall License





## Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct <sup>3</sup> , AI-based Heuristic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video <sup>3</sup> Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention <sup>3</sup>	•	•		
	Data Loss Prevention (DLP) <sup>1</sup>	•	•		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	•	•		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS <sup>1</sup>	•			
	Application Control			included with FortiCare Subscription	
Inline CASB <sup>3</sup>			included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring	•			
	SD-WAN Overlay-as-a-Service	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth) <sup>2</sup>	•			
NOC and SOC Services	FortiConverter Service for one time configuration conversion	•	•		
	Managed FortiGate Service—available 24×7, with Fortinet NOC experts performing device setup, network, and policy change management	•			
	FortiGate Cloud—Management, Analysis, and One Year Log Retention	•			
	FortiManager Cloud	•			
	FortiAnalyzer Cloud	•			
	FortiGuard SOCaaS—24×7 cloud-based managed log monitoring, incident triage, and SOC escalation service	•			
Hardware and Software Support	FortiCare Essentials <sup>2</sup>	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Device/OS Detection, GeolIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing		included with FortiCare Subscription		

1. Full features available when running FortiOS 7.4.1.

2. Desktop Models only.

3. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards.



### FortiGuard Bundles

FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24×7×365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.

## Ordering Information

Product	SKU	Description
FortiGate 3500F	FG-3500F	6× 100GE/ 40GE QSFP28 slots and 32× 25GE/ 10GE SFP28 slots, 2× 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, and 2 AC power supplies.
FortiGate 3501F	FG-3501F	6× 100GE/ 40GE QSFP28 slots and 32× 25GE/ 10GE SFP28 slots, 2× 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, 4 TB SSD onboard storage, and 2 AC power supplies.
Optional Accessories/Spares	SKU	Description
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-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC and FG-3950B/-DC.
AC Power Supply	FG-7040E-PS-AC	1500W AC Power Supply for FG-3500F, FG-3501F, FG-3700F, FG-3701F, FG-7030E, FG-7040E, FG-6000F, and FG-3900E series (not compatible for use with FG-7060E), does not include SP-FGPCORC15-XX power cord.
Transceiver Modules	SKU	Description
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for systems with SFP+ and SFP/SFP+ slots.
10Gbase-ER SFP+ transceivers	FN-TRAN-SFP+ER	10Gbase-ER SFP+ transceiver module, 1550nm Single Mode, 40km range for systems with SFP+ Slots.
10 GE SFP+ Transceiver Module, 80km Extreme Long Range	FN-TRAN-SFP+ZR	10 GE SFP+ transceiver module, 80km extreme long range, for systems with SFP+ and SFP/SFP+ slots.
25 GE SFP28 Transceiver Module, Short Range	FN-TRAN-SFP28-SR	25 GE SFP28 transceiver module, short range for systems with SFP28 slots.
25 GE SFP28 Transceiver Module, Long Range	FN-TRAN-SFP28-LR	25 GE SFP28 transceiver module, long range for systems with SFP28 slots.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short range for 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 systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, long range for systems with QSFP+ slots.
100 GE QSFP28 Transceiver Module, Short Range	FN-TRAN-QSFP28-SR	100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, Long Range	FN-TRAN-QSFP28-LR	100 GE QSFP28 transceivers, 4 channel parallel fiber, long range for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, CWDM4	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module	FN-TRAN-QSFP28-DR	100GE QSFP28 transceiver module, single channel single-mode fiber, 100GBase-DR for systems with QSFP28 slots.
100 GE QSFP28 BiDi Transceiver Module	FN-TRAN-QSFP28-BIDI	100 GE QSFP28 BiDi transceiver module, for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, 100m Range	FN-TRAN-QSFP28-SR4	100 GE QSFP28 transceiver module, 100m range, MMF, for systems with QSFP28 slots.
Cables	SKU	Description
25 GE SFP28 Passive Direct Attach Cable, 1m Range	FN-CABLE-SFP28-1	25 GE SFP28 passive direct attach cable, 1m range, for systems with SFP28 slots.
25 GE SFP28 Passive Direct Attach Cable, 3m Range	FN-CABLE-SFP28-3	25 GE SFP28 Passive Direct Attach Cable, 3m range, for systems with SFP28 slots.
25 GE SFP28 Passive Direct Attach Cable, 5m Range	FN-CABLE-SFP28-5	25 GE SFP28 Passive Direct Attach Cable, 5m range, for systems with SFP28 slots.
100 GE QSFP28 Passive Direct Attach Cable, 1m Range	FN-CABLE-QSFP28-1	100 GE QSFP28 passive direct attach cable, 1m range, for systems with QSFP28 slots.
100 GE QSFP28 Passive Direct Attach Cable, 2m Range	FN-CABLE-QSFP28-2	100 GE QSFP28 passive direct attach cable, 2m range, for systems with QSFP28 slots.
100 GE QSFP28 Passive Direct Attach Cable, 3m Range	FN-CABLE-QSFP28-3	100 GE QSFP28 passive direct attach cable, 3m range, for systems with QSFP28 slots.

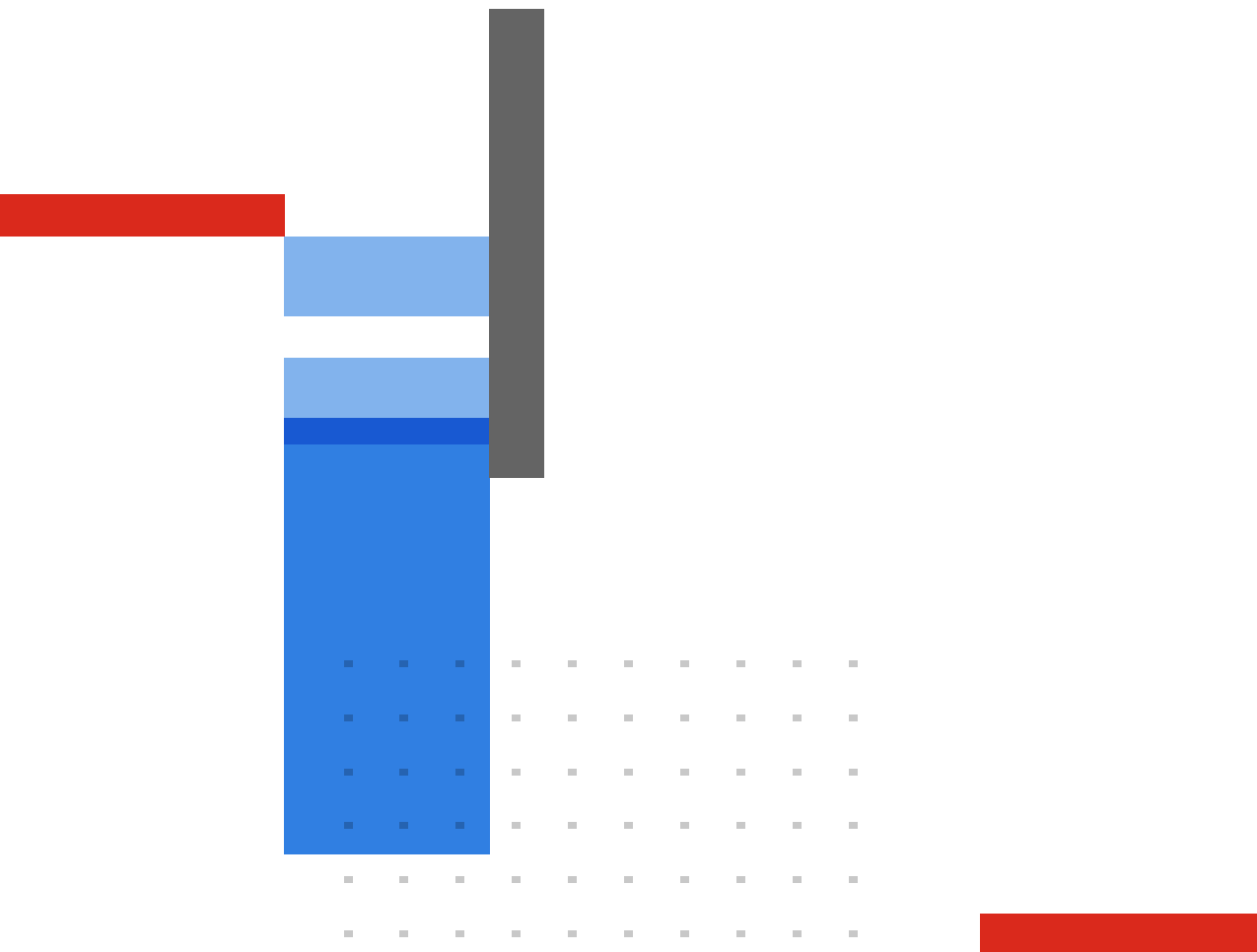
Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.



---

## Fortinet Corporate Social Responsibility 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](http://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 SVP Legal and above, 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.