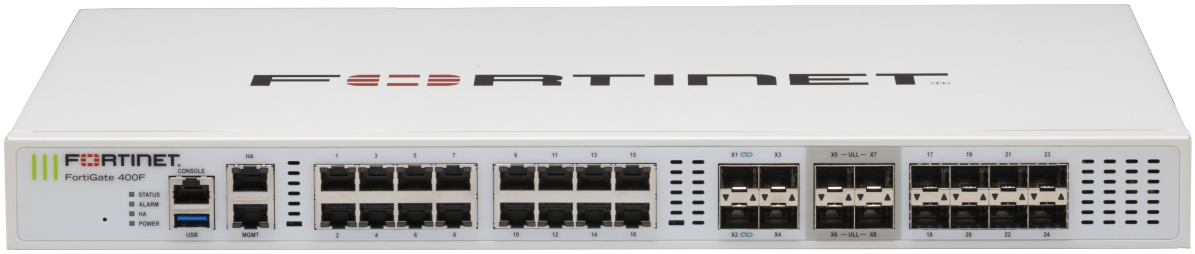
FortiGate 400F Series

FG-400F, FG-401F, FG-400F-DC, FG-401F-DC



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and WAN Edge Infrastructure.

Security-Driven Networking FortiOS delivers converged networking and security.

State-of-the-Art Unparalleled Performance with Fortinet's patented / SPU / vSPU processors.

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

Deep Visibility into applications, users, and devices beyond traditional firewall techniques.

AI/ML Security and Deep Visibility

The FortiGate 400F Series NGFW combines AI-powered security and machine learning to deliver Threat Protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 400F Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks.

Universal ZTNA automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users. Ultra-fast Threat Protection and SSL Inspection provides security at the edge you can see without impacting performance.

IPS	NGFW	Threat Protection	Interfaces
12 Gbps	10 Gbps	9 Gbps	Multiple GE RJ45, 10GE SFP+ Slots, GE SFP Slots

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.

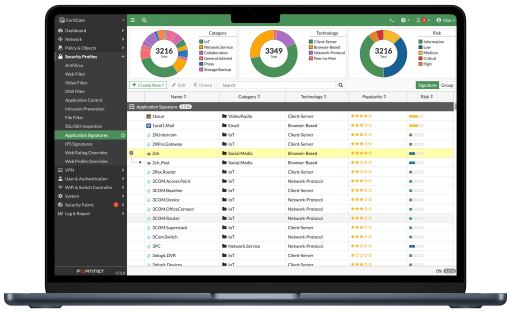
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

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 Migration 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

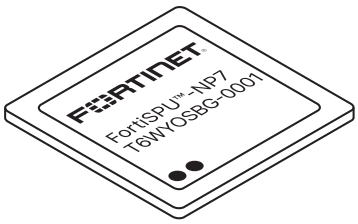
The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

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



Network Processor 7 NP7

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

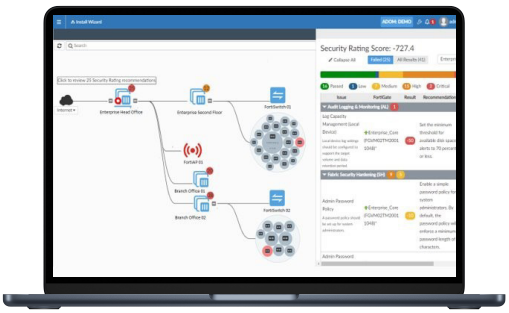
- Hyperscale firewall, accelerated session setup, and ultra-low latency
- Industry-leading performance for VPN, VXLAN termination, hardware logging, and elephant flows



Content Processor 9 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



Intuitive view and clear insights into network security posture with FortiManager

Centralized Network and Security Management at Scale

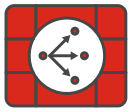
FortiManager, the centralized management solution from Fortinet, enables integrated management of the Fortinet security fabric, including devices like FortiGate, FortiSwitch, and FortiAP. It simplifies and automates the oversight of network and security functions across diverse environments, serving 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

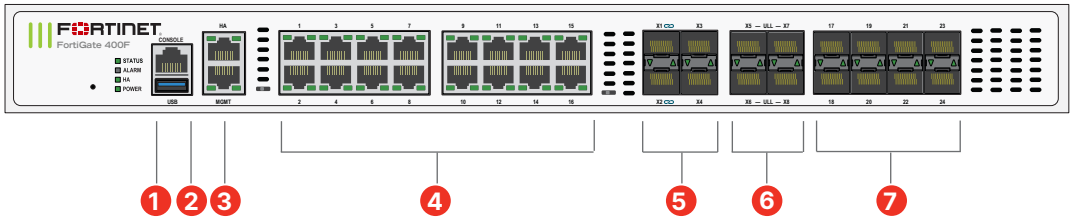


Segmentation

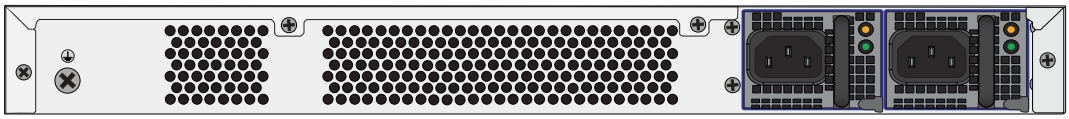
- Dynamic segmentation adapts to any network topology to deliver true end-to-end security—from the branch to the datacenter and across multi-cloud environments
- Ultra-scalable, low latency, VXLAN segmentation bridges physical and virtual domains with Layer 4 firewall rules
- Prevents lateral movement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

Hardware

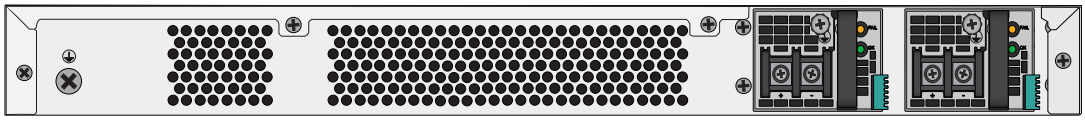
FortiGate 400F/401F/-DC Series Front Panel



FortiGate 400F/401F AC Series Rear Panel



FortiGate 400F/401F DC Series Rear Panel



Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/HA Ports
4. 16 x GE RJ45 Ports
5. 4 × 1GE/10GE SFP+ Slots
6. 4 × 10GE SFP+ Ultra Low Latency Slots
7. 8× 1GE SFP Slots

Hardware Features

NP7 CP9 TPM 1RU 10/GE DUAL AC 960GB DUAL DC

Trusted Platform Module (TPM)

The FortiGate 400F 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.

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

	FG-400F/-DC	FG-401F/-DC
Interfaces and Modules		
Hardware Accelerated GE RJ45 Interfaces	16	
Hardware Accelerated GE SFP Slots	8	
Hardware Accelerated 10GE SFP+ Slots	4	
Hardware Accelerated 10GE SFP+ Ultra Low Latency Slots	4	
GE RJ45 Management Ports	2	
USB Ports	1	
RJ45 Console Port	1	
Onboard Storage	0	2× 480 GB SSD
Trusted Platform Module (TPM)	Yes	Yes
Included Transceivers	2x SFP (SX 1 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	12 Gbps	
NGFW Throughput [2, 4]	10 Gbps	
Threat Protection Throughput [2, 5]	9 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	79.5 / 78.5 / 70 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	79.5 / 78.5 / 70 Gbps	
Firewall Latency (64 byte, UDP)	4.19 µs / 2.5 µs*	
Firewall Throughput (Packet per Second)	105 Mpps	
Concurrent Sessions (TCP)	7.8 Million	
New Sessions/Second (TCP)	500 000	
Firewall Policies	10 000	
IPsec VPN Throughput (512 byte) [1]	55 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	50 000	
SSL-VPN Throughput [6]	3.6 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	5000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	8 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	6000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	800 000	
Application Control Throughput (HTTP 64K) [2]	28 Gbps	
CAPWAP Throughput (HTTP 64K)	65 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	72	
Maximum Number of FortiAPs (Total / Tunnel)	512 / 256	
Maximum Number of FortiTokens	5000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-400F/-DC	FG-401F/-DC
Dimensions and Power		
Height x Width x Length (inches)	1.75 × 17.0 × 15.0	
Height x Width x Length (mm)	44.45 × 432 × 380	
Weight	14.11 lbs (6.4 kg)	14.33 lbs (6.5 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 1 RU	
AC Power Consumption (Average / Maximum)	154.8 W / 189.2 W	161.1 W / 196.9 W
AC Power Input	100–240V AC, 50/60Hz	
AC Current (Maximum)	6A	
DC Power Supply	48-60VDC	
DC Current (Maximum)	TBA	
Heat Dissipation	645.58 BTU/h	671.85 BTU/h
Power Supply Efficiency Rating	80Plus Compliant	
Redundant Power Supplies (Hot Swappable)	Yes (Default dual AC PSU for 1+1 Redundancy)	
Operating Environment and Certifications		
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	5% to 90% non-condensing	
Noise Level	LPA 48 dBA / LWA 55 dBA	
Airflow	Side and 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	

* Latency based on Ultra Low Latency (ULL ports)

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

			Bundles		
Service Category	Service Offering	A-la-carte	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 [3], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video [3] Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention [3]	•	•		
	Data Loss Prevention (DLP) [1]	•	•		
	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 [1]	•			
	Application Control		included with FortiCare Subscription		
	Inline CASB [3]		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) [2]	•			
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 [2]	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Device/OS Detection, GeoIPs, 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 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

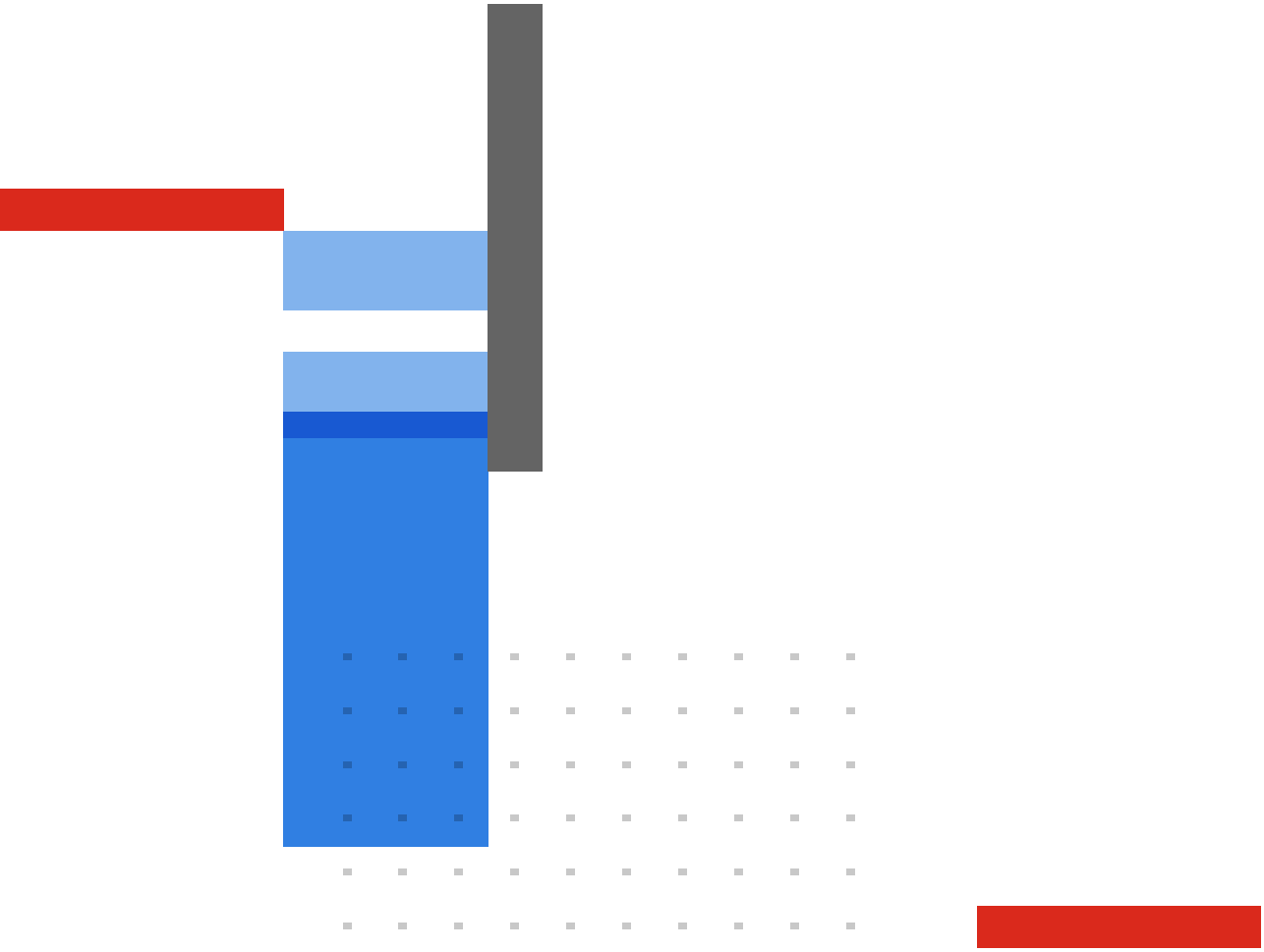
Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive lifecycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service variants, offers heightened SLAs and swift issue resolution 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 400F	FG-400F	18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, 8× 10GE SFP+ slots, SPU NP7 and CP9 hardware accelerated, dual AC power supplies.
FortiGate 400F-DC	FG-400F-DC	18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, 8× 10GE SFP+ slots, SPU NP7 and CP9 hardware accelerated, dual DC power supplies.
FortiGate 401F	FG-401F	18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, 8× 10GE SFP+ slots, SPU NP7 and CP9 hardware accelerated, 2× 480GB onboard SSD storage, dual AC power supplies.
FortiGate 401F-DC	FG-401F-DC	18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, 8× 10GE SFP+ slots, SPU NP7 and CP9 hardware accelerated, 960GB onboard SSD storage, dual DC power supplies.
Optional Accessories	**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.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for systems with SFP+ and SFP/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.
10 GE SFP+ Passive Direct Attach Cable, 1m Range	FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m range, for systems with SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 3m Range	FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m range, for systems with SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable, 5m Range	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m range, for systems with SFP+ slots.
AC Power Supply	SP-FG400F-PS	AC power supply for FG-400/401F, FG-600/601F, power cable SP-FGPCOR-XX sold separately.
DC Power Supply	SP-FG400F-DC-PS	DC power supply for FG-400/401F-DC and FG-900/901G-DC, comes with 3m DC cable.

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.



FORTINET

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.

July 10, 2024

FG-400F-DAT-R13-20240710