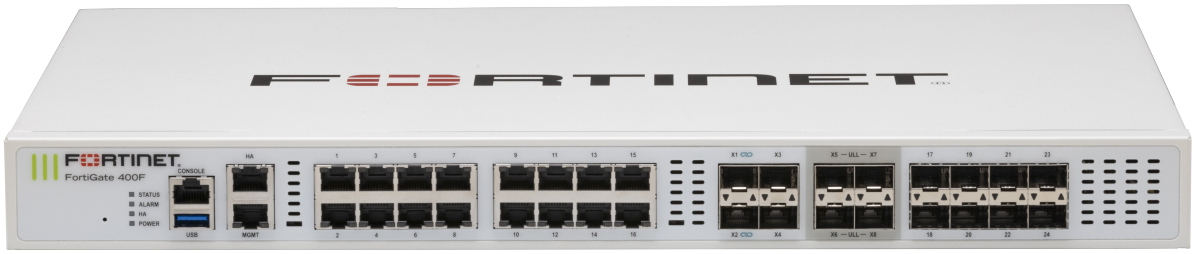
# FortiGate 400F Series



## Highlights

**Leader in the Gartner® Magic Quadrant™** for Hybrid Mesh Firewall

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

**State-of-the-art unparalleled performance** with Fortinet's patented SPU and vSPU processors

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

**Deep visibility** into applications, users, and devices beyond traditional firewall techniques

## Artificial Intelligence, Machine Learning Security with Deep Visibility

The FortiGate 400F series next-generation firewall (NGFW) combines artificial intelligence (AI)-powered security and machine learning (ML) 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. This security fabric seamlessly extends across your entire environment, including a Hybrid Mesh Firewall architecture, ensuring consistent policy enforcement and threat protection across all network segments.

Universal zero-trust network access (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 |

## 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

### 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

### 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 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

Available in

Appliance

Virtual

Hosted

Cloud

Container

## FortiOS Everywhere

**FortiOS, Fortinet's Real-Time Quantum-Safe Network Security Operating System**

FortiOS is Fortinet's natively AI-powered and quantum-safe operating system (OS) that powers the Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. It provides a unified framework for securing networks across on-premises, cloud, hybrid environments, and the convergence of IT, OT, and IoT.

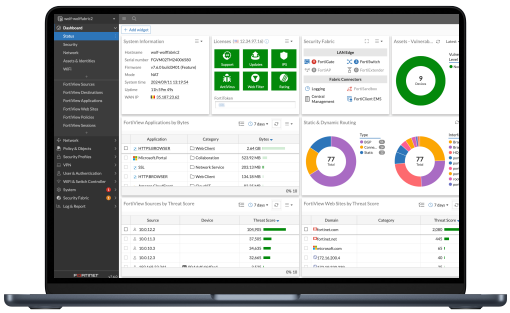
By converging networking and security functions into a single operating system, organizations can manage network and security more effectively to detect, investigate, and respond to incidents faster. This unified architecture simplifies operations, eliminates security silos, and allows organizations to scale securely without multiple tools or management complexity.

FortiOS also incorporates AI-driven capabilities that enhance threat detection, automate network activity analysis, and deliver more precise remediation guidance. Together, FortiGate firewalls and FortiOS provide intelligent, adaptive protection that reduces complexity, improves operational efficiency, and strengthens security across modern hybrid environments.

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*



## 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. Powered by real-time AI enhanced threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero days and evasive, sophisticated AI-powered attacks.

### Network and file security

Network and file security services protect against network and file-based threats. Consists of intrusion prevention system (IPS) which uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, uncovers hidden command-and-control activity, and applies virtual patches for newly discovered vulnerabilities. Application control improves security compliance and provides real-time visibility into applications and usage including generative AI (GenAI) applications.

### 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 millions of URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks.

### SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This service includes data loss/leakage prevention in files, GenAI applications and Images via OCR(optical character recognition). This ensures visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. The inline CASB service, secures SaaS applications in use, providing broad visibility and granular control over SaaS access, usage, and data.

### 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 and zero-day malware in real time, delivering sub-second protection across all NGFWs. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

### Attack surface visibility and compliance

The FortiGuard Attack Surface Security Service provides continuous, compliance-ready monitoring of your Fortinet Security Fabric infrastructure. It calculates your overall security posture rating by scoring controls against vulnerabilities, misconfigurations, and sub-optimal settings, while offering specific remediation guidelines for devices found out of configuration. It maintains continuous compliance with PCI DSS, CIS Controls, and Fortinet security best practices.

### OT security

With over 2400 virtual patches, 1600+ OT applications, and 3500+ 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.

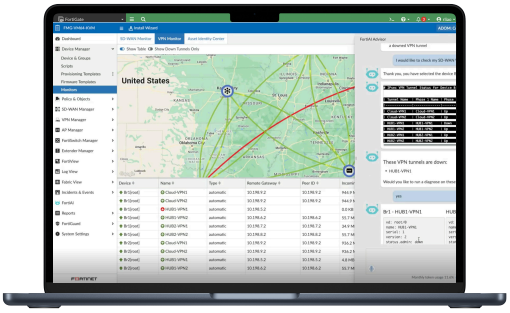
## FortiManager

**AI-Powered, Automation-Driven, Enterprise-Class Centralized Management at Scale**

FortiManager, powered by FortiAI-Assist, provides centralized, single-pane management for the Fortinet Security Fabric, unifying configuration, policy, and responses across thousands of devices. It converges networking and security management, enabling consistent policy enforcement across SD-WAN, ZTNA, SASE, and branch environments while delivering real-time visibility and automated network operations.

FortiAI-Assist helps with Day 0–1 provisioning and Day N troubleshooting and maintenance. AI agents collaborating via a unified Model Context Protocol (MCP) framework automates goal-driven tasks toward a self-healing operation.

FortiManager integrates with FortiSOC for contextual insights and fabric-wise response. It also supports ecosystem integrations, and open APIs for extended automation. ADOM-based administration and FortiManager clusters enables resilient control across distributed networks.



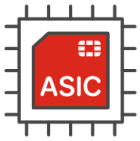

*GenAI in FortiManager helps manage networks effortlessly—generates configuration and policy scripts, troubleshoots issues, and executes recommended actions.*

## 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.

## 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

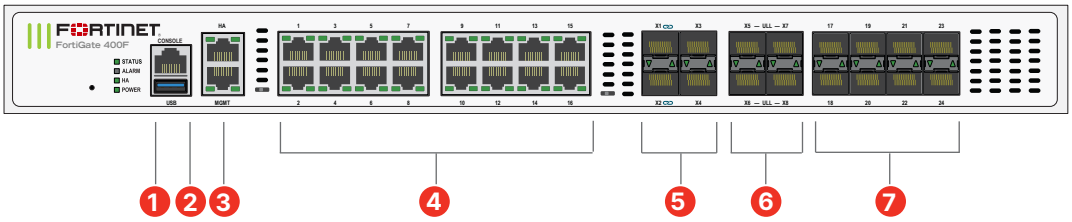
### Content processor CP9

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:

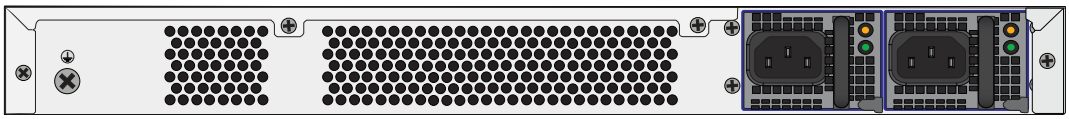
- Pattern matching acceleration and fast inspection of real-time traffic for application identification
- IPS pre-scan/pre-match, signature correlation offload, and accelerated antivirus processing

# Hardware

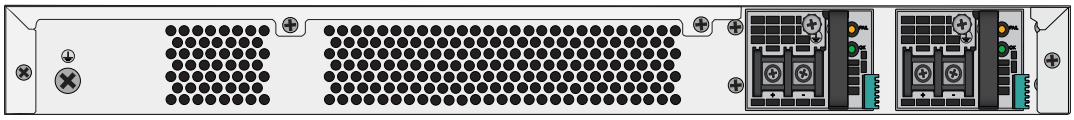
### FortiGate 400F/401F/-DC Series Front Panel




### 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.

#### Dual power supply

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 400F series offers dual hot swappable power supplies.

#### Access layer security

FortiLink protocol enables you to converge security and network access by integrating the FortiSwitch into the FortiGate as a logical extension of the firewall. 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) | ✓ | |
| Bluetooth Low Energy (BLE) | — | |
| Signed Firmware Hardware Switch | — | |
| 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 | 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 / 25 | |
| Maximum Number of FortiSwitches Supported | 96** | |
| 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) | 12A | |
| Heat Dissipation | 645.58 BTU/h | 671.85 BTU/h |
| Power Supply Efficiency Rating | 80Plus Compliant | |
| Redundant Power Supplies (Hot Swappable) | ✓ (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)

** FortiOS 7.6.1+ is required for supporting up to 96 FSW. All prior releases support up to 72.

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.

# Subscriptions

| Service Category | Service Offering | A-la-carte | Bundles: Enterprise Protection | Bundles: Unified Threat Protection | Bundles: Advanced Threat Protection | Bundles: SD-WAN |
|---|---|---|---|---|---|---|
| FortiGuard Security Services | IPS — IPS, Malicious/Botnet URLs | • | • | • | • | |
| | Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct, AI-based Heurestic AV, FortiGate Cloud Sandbox[1] | • | • | • | • | |
| | URL, DNS and Video Filtering — URL, DNS and Video Filtering, Malicious Certificate[1] | • | • | • | | |
| | Anti-Spam | | • | • | | |
| | AI-based Inline Malware Prevention | • | • | | | |
| | Data Loss Prevention (DLP)[2] | • | • | | | |
| | IoT Security — IoT Device Detection, IoT Vulnerability Correlation, and Virtual Patching[3] | | • | | | • |
| | Security Rating (and Outbreak Check)[3] | | • | | | • |
| | OT Security—OT Device Detection, OT Vulnerability Correlation and Virtual Patching, OT Application Control and IPS[2] | • | | | | |
| | Application Control | ----------included with FortiCare Subscription---------- | | | | |
| | Inline CASB[1] | ----------included with FortiCare Subscription---------- | | | | |
| SD-WAN and SASE Services | SD-WAN SLA Database | | | | | • |
| | SD-WAN Underlay and Application Monitoring Service | | | | | • |
| | SD-WAN Overlay Orchestration Service | | | | | • |
| | SD-WAN Connector for FortiSASE Secure Private Access | | | | | • |
| | FortiSASE Starter Kit for n* Users[4] | | | | | • |
| | One Year Cloud-based Log Retention | | | | | • |
| | FortiTelemetry Cloud | | | | | • |
| 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 | • | | | | |
| | FortiManagement 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 | Desktop models only | | | | |
| | FortiCare Premium[3] | • | • | • | • | • |
| | 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. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.
2. Full features available when running FortiOS 7.4.1.
3. Not available for SD-WAN Bundle SKU FC-10-XXXXX-1387-02-DD.
4. Only supported on FortiGate/FortiWiFi models from the 70F (F-series and all later series) and FGR-60G onwards. See the FortiSASE Ordering Guide for supported models and corresponding user license allocations.

FortiGuard AI-Powered Security Bundles offer curated security services to combat known, unknown, zero-day, and emerging AI threats. They protect against malicious content, web threats, and secure IT/OT/IoT devices, applications, users, and data. All bundles include FortiCare Premium Services with 24×7×365 support, one-hour critical response, and next-business-day noncritical response.

Fortinet's FortiCare Services support the Security Fabric throughout its lifecycle—Design, Deploy, Operate, Optimize, and Evolve. FortiCare Elite delivers enhanced SLAs, rapid issue resolution, dedicated support, 18 months of extended engineering support, and a unified portal for device and security health, improving operational efficiency and 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** |
| **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. |
| **Transceivers** | **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. |
| **1 GE SFP Transceiver Module, 90km range, -40/85c operation** | FR-TRAN-ZX | 1 GE SFP transceiver module, long range 90km, LC connector, SMF, 1550nm, -40°C to 85°C, for systems with 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. |
| **Cables** | **SKU** | **Description** |
| **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. |

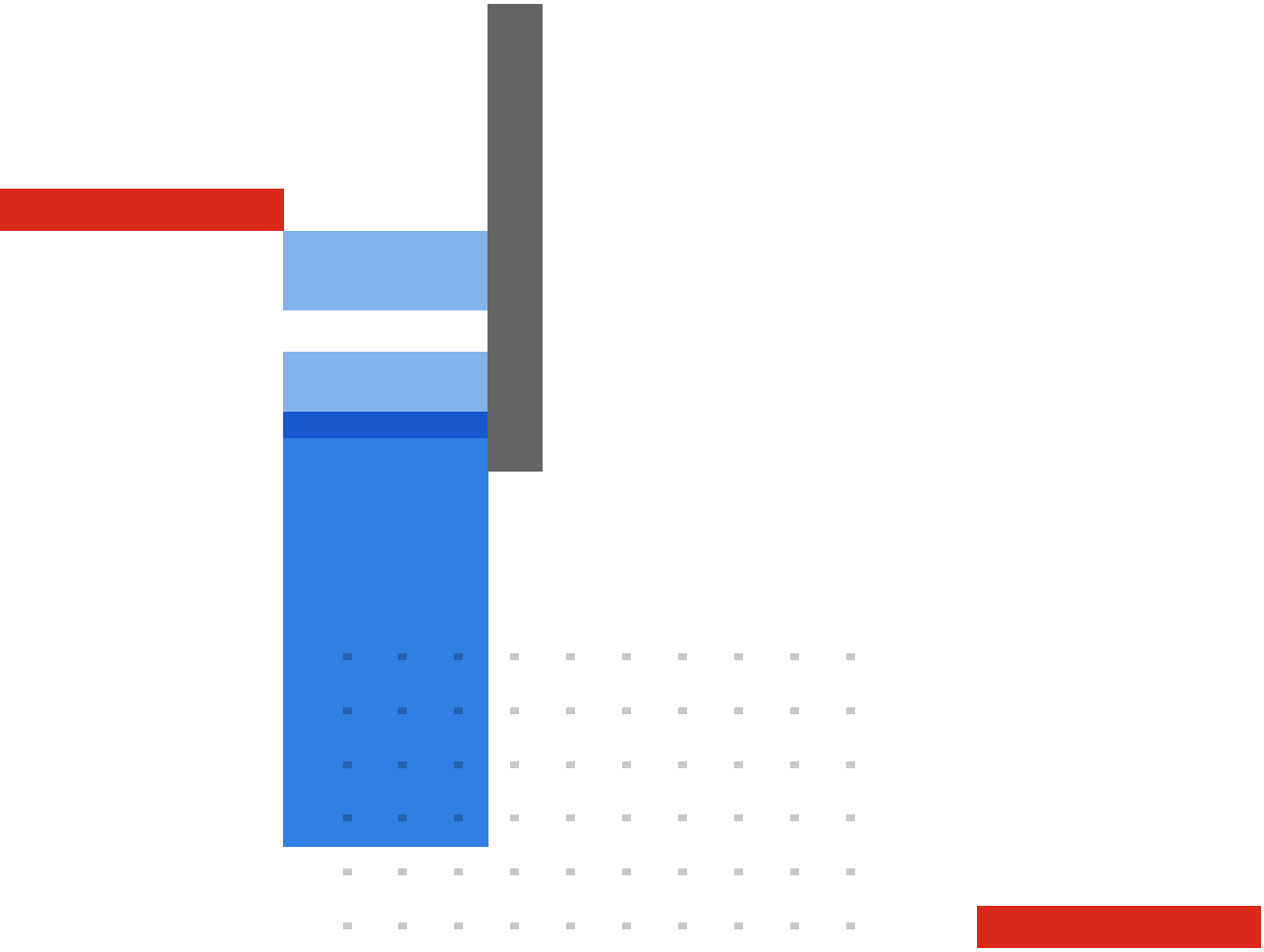
Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

For hard-coded firmware ceilings for a specific software version, visit: Maximum Values Table Tool.

The link to the max value table: https://docs.fortinet.com/max-value-table?product_family=fortigate&family=fortigate

## 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 © 2026 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.

October 1, 2026

FG-400F-DAT-R23-20261001