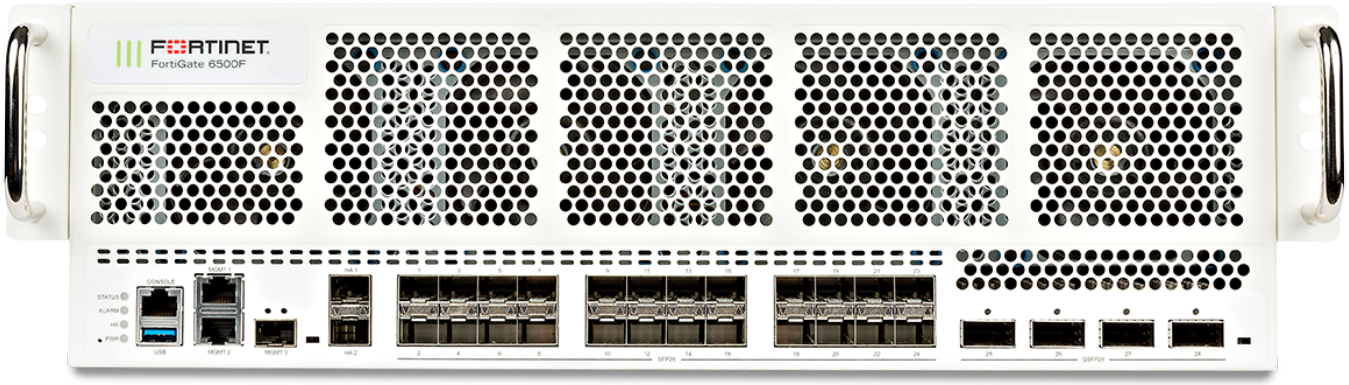
Data Sheet

FortiGate 6000F Series



Highlights

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

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 6000F Series enables organizations to build security-driven networks, forming the foundation of a robust Hybrid Mesh Firewall architecture. This approach weaves security deep into their datacenter and across their hybrid IT environment, protecting any edge at any scale.

Powered by a rich set of AI/ML-based FortiGuard Services and an integrated security fabric platform, the FortiGate 6000F 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, FortiGate 6000F automatically controls, verifies, and facilitates user access to applications, delivering consistent convergence with a seamless user experience across your distributed network.

The industry's first integrated zero-trust network access (ZTNA) enforcement within an NGFW solution, the FortiGate 6000F automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users for seamless user experience.

Model	IPS	NGFW	Threat Protection	Interfaces
6001F	51/17/170 Gbps	45/15/150 Gbps	30/10/100 Gbps	Multiple 40/100 GE QSFP28, 1/10/25 GE SFP28, 1/10 GE SFP+ and GE RJ45 slots
6300F/6301F	110 Gbps	90 Gbps	60 Gbps	Multiple 40/100 GE QSFP28, 1/10/25 GE SFP28, 1/10 GE SFP+ and GE RJ45 slots
6500F/6501F	170 Gbps	150 Gbps	100 Gbps	Multiple 40/100 GE QSFP28, 1/10/25 GE SFP28, 1/10 GE SFP+ and GE RJ45 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

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

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

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

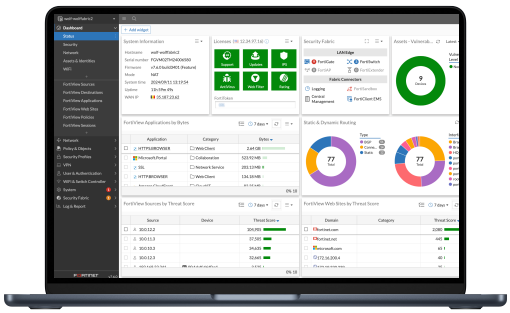
FortiOS is Fortinet's natively AI-powered and quantum-safe operating system (OS) that powers the Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. It provides a unified framework for securing networks across on-premises,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

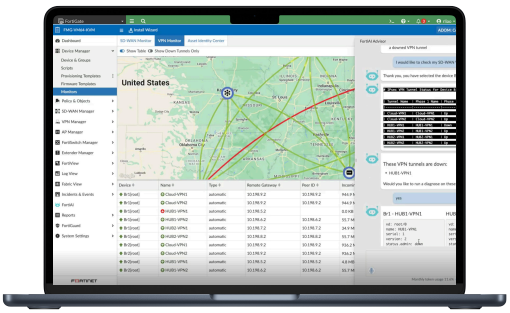
FortiManager

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

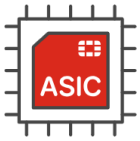
The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations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

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.

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 NP6

Fortinet's new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

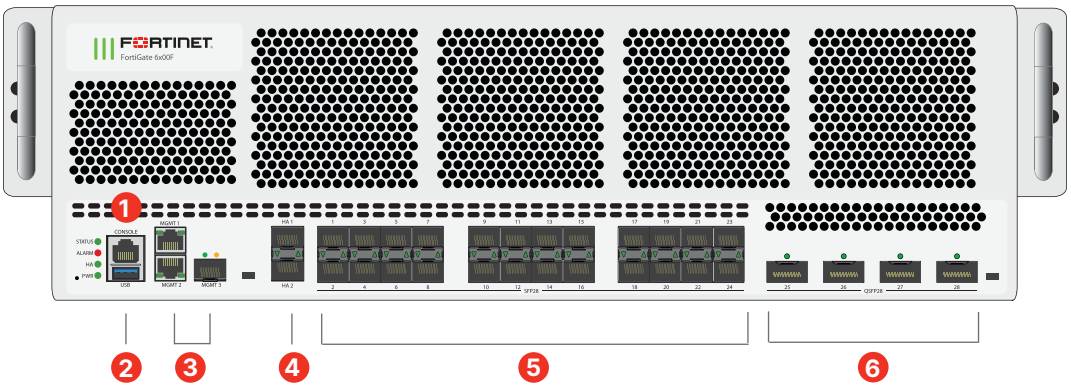
Content processor CP9

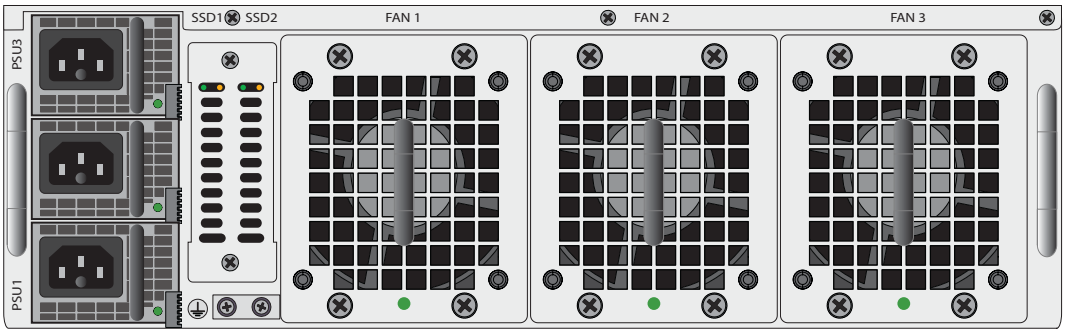
Content processors act as co-processors to offload resource-intensive processing of security functions. The ninth generation of the Fortinet Content Processor, the CP9, accelerates resource-intensive SSL (including TLS 1.3) decryption and security functions while delivering:

- 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 FG-6001, FG-6300F/-DC, FG-6301F/-DC, FG-6500F/-DC, FG-6501F/-DC





Interfaces

1. Console Port
2. USB Port
3. 2 x GE RJ45, 1 X 1/10 GE SFP+ Management Ports
4. 2 × 10 GE SFP+ HA Slots
5. 24 × 1/10/25 GE SFP/SFP+/SFP28 Slots
6. 4 × 40/100 GE QSFP+/QSFP28 Slots

Hardware Features

NP6 | CP9 | DP3 | 3RU | 100/40/25/GE | FortiCarrier | 2×960GB NVMe

FG-6001F Configuration

The FG-6001F comes with 10x FPC blades installed by default and an embedded license to enable 3x FPC blades only. If higher throughput is required, an additional perpetual license or subscription license is available to enable more FPC blades for increased throughput.

Specifications

FORTIGATE	6001F	6300F/-DC, 6301F/-DC	6500F/-DC, 6501F/-DC
Interfaces and Modules			
Hardware Accelerated 40/100 GE QSFP28 Slots		4	
Hardware Accelerated 1/10/25 GE SFP28 Slots		24	
Hardware Accelerated 10 GE SFP+ Slots		3	
GE RJ45 Management Ports		2	
USB Port		1	
Console Port		1	
Onboard Storage	2× 960 GB NVMe	— 2× 960 GB NVMe	— 2× 960 GB NVMe
Trusted Platform Module (TPM)		—	
Bluetooth Low Energy (BLE)		—	
Signed Firmware Hardware Switch		—	
Included Transceivers		2x SFP+ (SR 10 GE)	
System Performance — Enterprise Traffic	**MixDefault/ per FPC / Max**		
IPS Throughput [2]	51 / 17 / 170 Gbps	110 Gbps	170 Gbps
NGFW Throughput [2, 4]	45 / 15 / 150 Gbps	90 Gbps	150 Gbps
Threat Protection Throughput [2, 5]	30 / 10 / 100 Gbps	60 Gbps	100 Gbps
System Performance and Capacity			
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	1518: 120 / 40 / 239 Gbps 512: 120 / 40 / 238 Gbps 1518: 40.5 / 13.5 / 135 Gbps	239 / 238 / 135 Gbps	239 / 238 / 135 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)		239 / 238 / 135 Gbps	239 / 238 / 135 Gbps
Firewall Latency (64 byte, UDP)	4.80 µs	4.80 µs	4.80 µs
Firewall Throughput (Packet per Second)	60.75 / 20.25 / 202.5 Mpps	202.5 Mpps	202.5 Mpps
Concurrent Sessions (TCP)	60 / 20 / 200 Million	120 Million	200 Million
New Sessions/Second (TCP)	900 000 / 300 000 / 3 Million	2 Million	3 Million
Firewall Policies	200 000	200 000	200 000
IPsec VPN Throughput (512 byte) [1]	48 / 16 / 160 Gbps	96 Gbps	160 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	16 000	16 000	16 000
Client-to-Gateway IPsec VPN Tunnels	90 000	90 000	90 000
SSL-VPN Throughput	9 Gbps on Master FPC	9 Gbps	9 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30 000	30 000	30 000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	33 / 11 / 110 Gbps	66 Gbps	110 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	15 000 / 5000 / 50 000	30 000	50 000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	5.4 / 1.8 / 18 Million	10 Million	18 Million
Application Control Throughput (HTTP 64K) [2]	66 / 22 / 220 Gbps	150 Gbps	220 Gbps
CAPWAP Throughput (HTTP 64K)		N/A	
Virtual Domains (Default / Maximum)		10 / 500	
Maximum Number of FortiSwitches Supported		256	
Maximum Number of FortiAPs (Total / Tunnel)		N/A	
Maximum Number of FortiTokens		20 000	
High Availability Configurations		Active-Active (FGSP), Active-Passive, Clustering	

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

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

Specifications

FORTIGATE	6001F	6300F/-DC, 6301F/-DC	6500F/-DC, 6501F/-DC
Dimensions and Power			
Height x Width x Length (inches)	5.3 × 17.2 × 27.3	5.20 × 17.20 × 26.18	5.3 × 17.2 × 27.3
Height x Width x Length (mm)	133 × 437 × 694	132 × 437 × 665	133 × 437 × 694
Weight	78.26 lbs (35.5 kg) 79.59 lbs (36.1 kg)	67.68 lbs (30.7 kg) 69.00 lbs (31.3 kg)	78.26 lbs (35.5 kg) 79.59 lbs (36.1 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 3 RU		
AC Power Supply	100–240V AC, 50/60 Hz	100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	1308 W / 1548 W 1328 W / 1568 W	977 W / 1217 W 977 W / 1237 W	1308 W / 1548 W 1328 W / 1568 W
AC Current (Maximum)	30A@100VAC, 20A@240VAC		
DC Power Supply	N/A	-48 to -60V DC	
DC Current (Maximum)	N/A	25-32A (x2)	
Heat Dissipation	5282 BTU/h / 5350 BTU/h	4153 BTU/h / 4221 BTU/h	5282 BTU/h / 5350 BTU/h
Power Supply Efficiency Rating	80Plus Compliant		
Redundant Power Supplies	2+1 Redundant / 1+1 Redundant if using high line power Hot Swappable		
Fan Trays	Hot Swappable		
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	10% to 90% non-condensing		
Noise Level	57.43 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		

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[1], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•	
	URL, DNS and Video Filtering — URL, DNS and Video[1] Filtering, Malicious Certificate	•	•	•		
	Anti-Spam		•	•		
	AI-based Inline Malware Prevention	•	•			
	Data Loss Prevention (DLP) [2]	•	•			
	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 [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[3]					•
	FortiGate Cloud 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	•				
	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	Desktop models only				
	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. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.
2. Full features available when running FortiOS 7.4.1.
3. Only supported on FortiGate models from the 100F onwards (F-series and all later series).
See the FortiSASE Ordering Guide for supported models and corresponding user license allocations.

FortiGuard AI-Powered Security Bundles for FortiGate

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
Hardware		
FortiGate 6001F	FG-6001F	4× 40/100GE QSFP28 slots, 24× 1/10/25GE SFP28 slots, 2× 1GE RJ45 management ports, 2× 1/10GE SFP+ HA slots, 1× 1/10GE SFP+ MGMT slot, 2× 960GB NVMe, and 3x AC power supplies (3FPC slots enabled by default, upgrade SKU LIC-FG6KF-FPC or FG-10-F6KF01-XXX-12).
FortiGate 6300F	FG-6300F	4× 40/100GE QSFP28 slots, 24× 1/10/25GE SFP28 slots, 2× 1GE RJ45 management ports, 2× 1/10GE SFP+ HA slots, 1× 1/10GE SFP+ MGMT slot, and 3x AC power supplies.
FortiGate 6300F-DC	FG-6300F-DC	4× 40/100GE QSFP28 slots, 24× 1/10/25GE SFP28 slots, 2× 1GE RJ45 management ports, 2× 1/10GE SFP+ HA slots, 1× 1/10GE SFP+ MGMT slot, and 2x DC power supplies.
FortiGate 6301F	FG-6301F	4× 40/100GE QSFP28 slots, 24× 1/10/25GE SFP28 slots, 2× 1GE RJ45 management ports, 2× 1/10GE SFP+ HA slots, 1× 1/10GE SFP+ MGMT slot, 2× 960 GB NVMe, and 3x AC power supplies.
FortiGate 6301F-DC	FG-6301F-DC	4× 40/100GE QSFP28 slots, 24× 1/10/25GE SFP28 slots, 2× 1GE RJ45 management ports, 2× 1/10GE SFP+ HA slots, 1× 1/10GE SFP+ MGMT slot, 2× 960 GB NVMe, and 2x DC power supplies.
FortiGate 6500F	FG-6500F	4× 40/100GE QSFP28 slots, 24× 1/10/25GE SFP28 slots, 2× 1GE RJ45 management ports, 2× 1/10GE SFP+ HA slots, 1× 1/10GE SFP+ MGMT slot, and 3x AC power supplies.
FortiGate 6500F-DC	FG-6500F-DC	4× 40/100GE QSFP28 slots, 24× 1/10/25GE SFP28 slots, 2× 1GE RJ45 management ports, 2× 1/10GE SFP+ HA slots, 1× 1/10GE SFP+ MGMT slot, and 2x DC power supplies.
FortiGate 6501F	FG-6501F	4× 40/100GE QSFP28 slots, 24× 1/10/25GE SFP28 slots, 2× 1GE RJ45 management ports, 2× 1/10GE SFP+ HA slots, 1× 1/10GE SFP+ MGMT slot, 2× 960 GB NVMe, and 3x AC power supplies.
FortiGate 6501F-DC	FG-6501F-DC	4× 40/100GE QSFP28 slots, 24× 1/10/25GE SFP28 slots, 2× 1GE RJ45 management ports, 2× 1/10GE SFP+ HA slots, 1× 1/10GE SFP+ MGMT slot, 2× 960 GB NVMe, and 2x DC power supplies.
Subscriptions		
Perpetual FPC License for FortiGate-6001F	LIC-FG6KF-FPC	Upgrade License to enable 1x FPC on FortiGate-6001F limited to 7 FPC capacity.
Annual subscription for FPC License	FC1-10-6KF01-XXX	Subscription License for enabling 1x FPC on FortiGate-6001F. This is a seat SKU where the total number of FPCs must be added as seats in an increment of one and the maximal order is seven FPCs.
Training		
FortiGate Chassis-based Firewall Platform (FGT 6000 series) Training - 2 days	FT-FGT-CHS-6K	Course description: https://training.fortinet.com/local/staticpage/view.php?page=library_fortigate-6000-series Upcoming sessions: https://training.fortinet.com/calendar/view.php/Course:FortiGate_6000_Series Price includes lab access and course material (Lab and Study guides). Exam voucher not included.
Optional Accessories/Spares		
Fan Tray	SP-FG4K6K-FAN	Spare Hot Swappable Fan Module for FG-420xF/440xF/6000F.
AC 1500W Power Supply	FG-7040E-PS-AC	1500W AC Power Supply for FG-7030E,FG-7040E, 6000F and FG-3900E series (not compatible for use with FG-7060E) , does not include SP-FGPCORC15-XX power cord.
AC 2000W Power Supply	SP-FG4000F-PS	2000W AC power supply for 4000F and 6000F series, does not include SP-FGPCORC15-XX power cord.
DC Power Supply	SP-FG4000F-DC-PS	DC power supply for FG-4200F-DC/4201F-DC, FG-4400F-DC/4401F-DC and FG-6000F-DC.
Power Cord	SP-FGPCORC15-XX	6 ft power cord, 15A125V XXX, PSE BLACK ROHS-6, for FG-3900E, 4000F, 6000F,W and 7000E/F Series.
Transceiver Modules		
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE Copper SFP+ RJ45 Transceiver (30m range)	FN-TRAN-SFP+GC	10 GE copper SFP+ RJ45 Fortinet Transceiver (30m range) for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, short range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all 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 all systems with SFP+ and SFP/SFP+ slots.
10 Gbase-ER SFP+ Transceivers	FN-TRAN-SFP+ER	10 Gbase-ER SFP+ transceivers for FortiSwitch and FortiGate, 1550nm. Single Mode. 40km range for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, 30km Long Range	FN-TRAN-SFP+BD27	10 GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately).
10 GE SFP+ Transceiver Module, 30 km long range	FN-TRAN-SFP+BD33	10 GE SFP+ transceiver module, 30KM long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
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/10GE Dual Rate SFP28 transceiver module, short range for all systems with SFP28/SFP+ slots.
25 GE SFP28 Transceiver Module, long range	FN-TRAN-SFP28-LR	25 GE SFP28 transceiver module, long range for all systems with SFP28 slots.

Ordering Information

Product	SKU	Description
40 GE QSFP+ Transceiver Module, short range	FN-TRAN-QSFP+SR	40GE QSFP+ transceivers, short range 40GE QSFP+ transceiver module, short range for systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, long range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceivers, long range for all 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 all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, 40km Extended Range	FN-TRAN-QSFP+ER	40 GE QSFP+ transceiver module, 40km extended range, for systems with QSFP+/QSFP28 slots.
100 GE QSFP28 Transceiver Module	FN-TRAN-QSFP28-SR	100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all 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 all systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 slots.
100 GE QSFP28 BIDI Transceiver Module	FN-TRAN-QSFP28-BIDI	100 GE QSFP28 BIDI transceiver module, 100m MMF LC connector, for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, short range BiDi	FN-TRAN-QSFP28-BIDI-I	100 GE QSFP28 BIDI transceiver module, short range, for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, 20km Extended Range	FN-TRAN-QSFP28-ER	100 GE QSFP28 transceiver module, 20km extended range, eLR4, gen3, for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, 20km Range	FN-TRAN-QSFP28-LR4	100 GE QSFP28 transceiver module, 20km range, LR4, 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.
Cables		
25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-SFP28-1	25 GE SFP28 passive direct attach cable 1m for systems with SFP28 slots.
25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-SFP28-3	25 GE SFP28 passive direct attach cable 3m for systems with SFP28 slots.
25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-SFP28-5	25 GE SFP28 passive direct attach cable 5m for systems with SFP28 slots.
40 GE QSFP+ Passive Direct Attach Cable, 1m Range	SP-CABLE-FS-QSFP+1	40 GE QSFP+ Passive Direct Attach Cable, 1m range for Systems with QSFP+ slots.
40 GE QSFP+ Passive Direct Attach Cable, 3m Range	SP-CABLE-FS-QSFP+3	40 GE QSFP+ Passive Direct Attach Cable, 3m range, for Systems with QSFP+ slots.
40 GE QSFP+ Passive Direct Attach Cable, 5m Range	SP-CABLE-FS-QSFP+5	40 GE QSFP+ Passive Direct Attach Cable, 5m range, for Systems with QSFP+ slots.
100 GE QSFP28 breakout to 4× 25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-QSFP28-4SFP28-1	100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable, 1m.
100 GE QSFP28 breakout to 4× 25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-QSFP28-4SFP28-3	100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable, 3m.
100 GE QSFP28 breakout to 4× 25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-QSFP28-4SFP28-5	100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable, 5m.
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.

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.

April 15, 2026

FG-6000F-DAT-R42-20260415