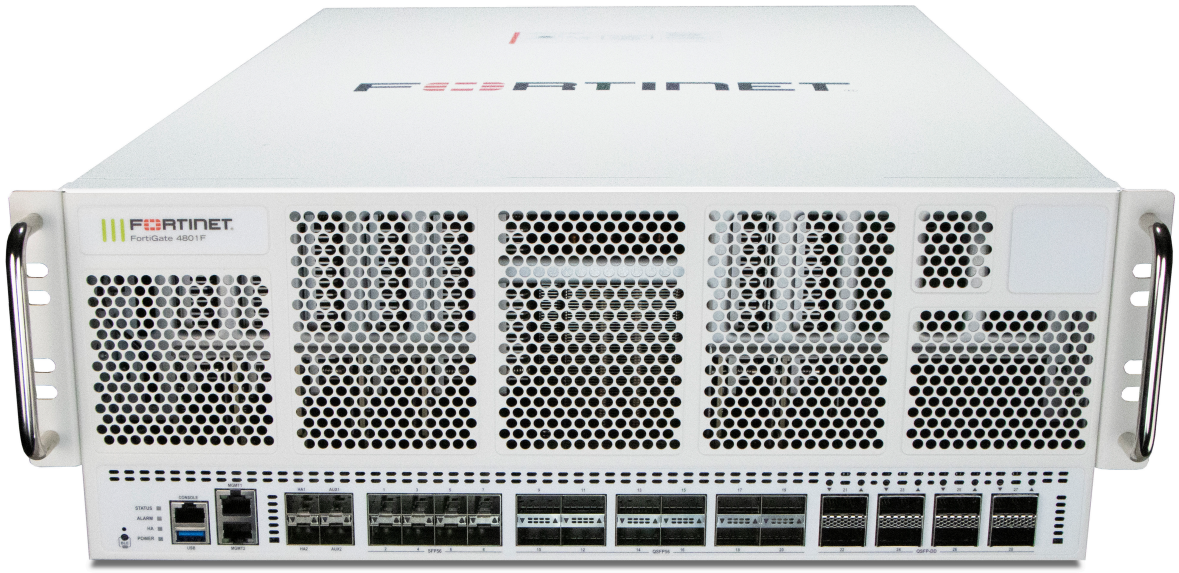
FortiGate 4800F Series



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 4800F 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 4800F 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 4800F 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 4800F 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
87 Gbps	77 Gbps	75 Gbps	Multiple 400GE/200GE QSFP-DD, 200GE/100GE/40GE, QSFP56/28, 50GE/25GE/10GE SFP65/28 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

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.

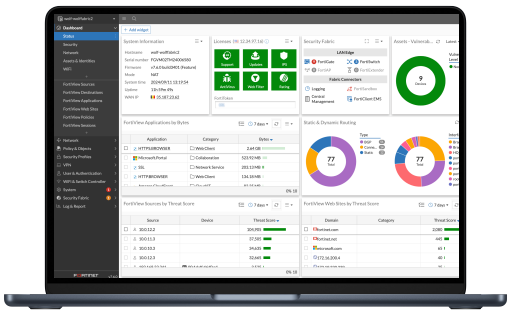
By converging networking and security functions into a single operating system, organizations can manage network and security more effectively to detect, investigate, and respond to incidents faster. This unified architecture simplifies operations, eliminates security silos, and allows organizations 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.

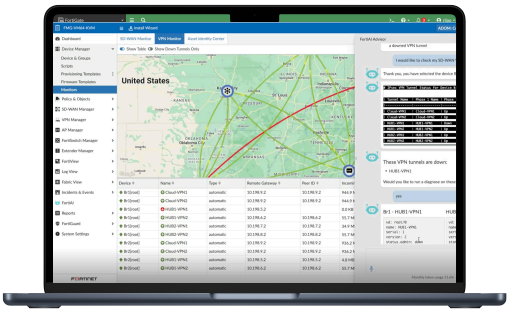
FortiManager

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.



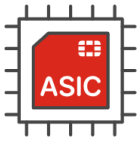
GenAI in FortiManager helps manage networks effortlessly—generates configuration and policy scripts, troubleshoots issues, and executes recommended actions.

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

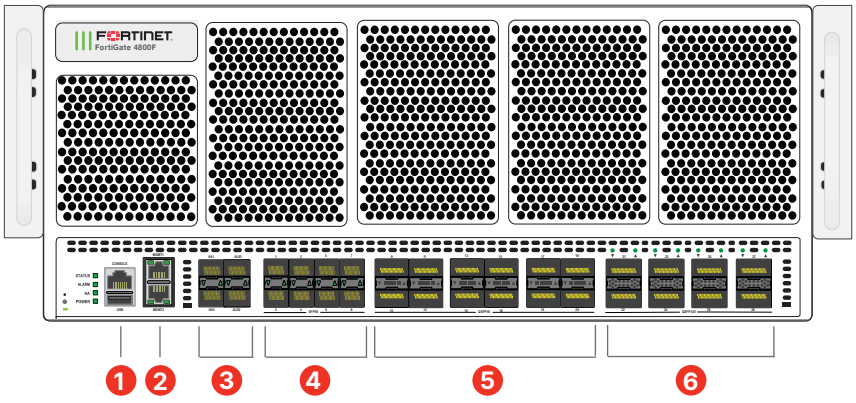
Content processor CP9

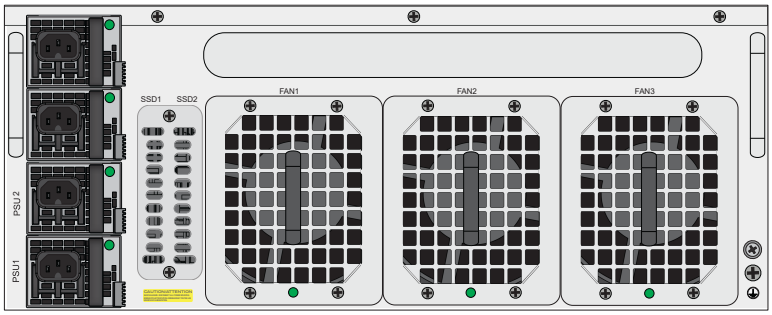
Content processors act as co-processors to offload resource-intensive processing of security functions. The ninth generation of the Fortinet Content Processor, the CP9, accelerates resource-intensive SSL (including TLS 1.3) decryption and security functions while delivering:

- 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 4800F/4801F Series





Interfaces

1. USB Management and Console Port
2. 2 × 10GE/GE RJ45 Management Ports
3. 4× 50GE/25GE/10GE/GE SFP56/SFP28/SFP+/SFP High Availability and Aux Slots
4. 8× 50GE/25GE/10GE/GE SFP56/SFP28/SFP+/SFP Slots
5. 12× 200GE/100GE/40GE QSFP56/QSFP28/QSFP+ Slots
6. 8× 400GE/200GE/100GE/40GE QSFP-DD/QSFP56/QSFP28/QSFP+ Slots

Hardware Features

NP7 CP9 4RU
100/40/25/10/GE 4x AC
Hyperscale
FortiCarrier
4TB 2×1.92TB

Hyperscale Firewall License

Empower organizations by unlocking further performance boosts with this perpetual license. The Hyperscale Firewall License will enable the hardware acceleration of CGNAT features by utilizing the latest SPU NP7. These features include hardware session setup, firewall session logging, and NAT.

Trusted Platform Module (TPM)

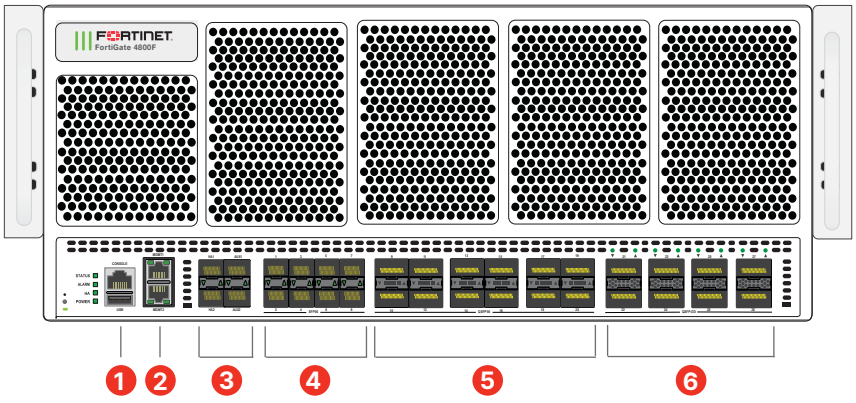
The FortiGate 4800F Series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.

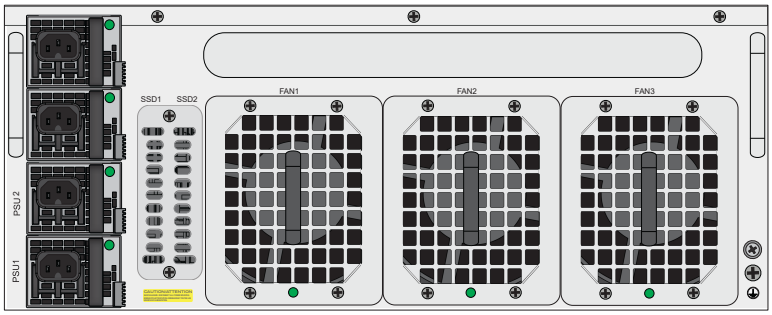
400 GE Connectivity for Network

High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 4800F Series provides multiple 400GE/200GE QSFP-DD slots, simplifying network designs without relying on additional devices to bridge desired connectivity.

Hardware

FortiGate 4801F-DC-NEBS and FortiGate 4801F-NEBS





Interfaces

1. USB Management and Console Port
2. 2 × 10GE/GE RJ45 Management Ports
3. 4× 50GE/25GE/10GE/GE SFP56/SFP28/SFP+/SFP High Availability and Aux Slots
4. 8× 50GE/25GE/10GE/GE SFP56/SFP28/SFP+/SFP Slots
5. 12× 200GE/100GE/40GE QSFP56/QSFP28/QSFP+ Slots
6. 8× 400GE/200GE/100GE/40GE QSFP-DD/QSFP56/QSFP28/QSFP+ Slots

Hardware Features

NP7 CP9 4RU
100/40/25/10/GE 4x AC
Hyperscale
FortiCarrier
2×1.92TB + NEBS

Hyperscale Firewall License

Empower organizations by unlocking further performance boosts with this perpetual license. The Hyperscale Firewall License will enable the hardware acceleration of CGNAT features by utilizing the latest SPU NP7. These features include hardware session setup, firewall session logging, and NAT.

Trusted Platform Module (TPM)

The FortiGate 4800F 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.

400 GE Connectivity for Network

High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 4800F Series provides multiple 400GE/200GE QSFP-DD slots, simplifying network designs without relying on additional devices to bridge desired connectivity.

Specifications

FORTIGATE	4800F/4800F-DC	4801F/4801F-DC	4801F-NEBS/4801F-DC-NEBS
Interfaces and Modules			
Hardware Accelerated 400GE/200GE/100GE/40GE QSFP-DD/ QSFP56/QSFP28/QSFP+ Slots	8	8	8
Hardware Accelerated 200GE/100GE/40GE QSFP56/QSFP28/QSFP+ slots	12	12	12
Hardware Accelerated 50GE/25GE/10GE/GE SFP56/SFP28/SFP+/SFP slots	8	8	8
Hardware Accelerated 50GE/25GE/10GE/GE SFP56/SFP28/SFP+/SFP High Availability and Aux Slots	4	4	4
10GE/GE RJ45 Management Ports	2	2	2
USB Port (3.0)	1	1	1
Console Port	1	1	1
Onboard Storage	—	2× 1.92TB SSD	2× 1.92TB SSD
Trusted Platform Module (TPM)	✓	✓	✓
Bluetooth Low Energy (BLE)	✓	✓	✓
Signed Firmware Hardware Switch	—	—	—
Included Transceivers	2x SFP+ (SR 10 GE)	2x SFP+ (SR 10 GE)	2x SFP+ (SR 10 GE)
System Performance — Enterprise Traffic Mix			
IPS Throughput [2]		87 Gbps	
NGFW Throughput [2, 4]		77 Gbps	
Threat Protection Throughput [2, 5]		75 Gbps	
System Performance and Capacity			
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)		3.1 / 3.1 / 0.93 Tbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)		3.1 / 3.1 / 0.93 Tbps	
Firewall Latency (64 byte, UDP)		3.6 µs	
Firewall Throughput (Packet per Second)		1396 Mpps	
Concurrent Sessions (TCP)		280 Million / 1.8 Billion *	
New Sessions/Second (TCP)		915 000 / 25 Million *	
Firewall Policies		200 000	
IPsec VPN Throughput (512 byte) [1]		800 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels		40 000	
Client-to-Gateway IPsec VPN Tunnels		200 000	
SSL-VPN Throughput[6]		18 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		30 000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]		63 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]		60 000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]		30 Million	
Application Control Throughput (HTTP 64K) [2]		180 Gbps	
CAPWAP Throughput (HTTP 64K)		112 Gbps	
Virtual Domains (Default / Maximum)		10 / 500	
Maximum Number of FortiSwitches Supported		300	
Maximum Number of FortiAPs (Total / Tunnel)		8192 / 4096	
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.

[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.

Specifications

FORTIGATE	4800F/4800F-DC	4801F/4801F-DC	4801F-NEBS/4801F-DC-NEBS
Dimensions and Power			
Height x Width x Length (inches)		6.89 × 17.13 × 26.10	
Height x Width x Length (mm)		175 × 435 × 663	
Weight	90.83 lbs (41.2 kg)	90.83 lbs (41.2 kg)	93.03 lbs (42.2 kg)
Form Factor (supports EIA/non-EIA standards)		Rack Mount, 4 RU	
AC Power Supply		200–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	1602 W / 1918.2 W	1622 W / 1938.2 W	1528.8W/ 1964.9W
AC Current (Maximum)	7.99A@240VAC	8.08A@240VAC	40.94A@-48VDC
Heat Dissipation	6544.9 BTU/h	6613.14 BTU/h	6700.31 / 6711.31 BTU/h
DC Power Input		-72V to -40V	
DC Current (Maximum)		40.94A@48VDC	
Redundant Power Supplies		✓ Hot Swappable, 2+2	
Power Supply Efficiency Rating		80Plus Compliant	
Fan Tray		Hot Swappable	
Operating Environment and Certifications			
Operating Temperature		32°F to 122°F (0°C to 50°C)	
Storage Temperature		-31°F to 158°F (-35°C to 70°C)	
Humidity		10% to 90% non-condensing	
Noise Level		63.794 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

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

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

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

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

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

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

[6] Uses RSA-2048 certificate.

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles			
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection	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 4800F	FG-4800F	8× 400GE/200GE QSFP-DD slots, 12× 200GE/100GE/40GE QSFP56/28 slots and 12× 50GE/25GE/10GE SFP56/28 slots, 2 × 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, and 4 AC power supplies.
FortiGate 4800F-DC	FG-4800F-DC	8× 400GE/200GE QSFP-DD slots, 12× 200GE/100GE/40GE QSFP56/28 slots and 12× 50GE/25GE/10GE SFP56/28 slots, 2 × 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, and 4x DC power supplies.
FortiGate 4801F	FG-4801F	8× 400GE/200GE QSFP-DD slots, 12× 200GE/100GE/40GE QSFP56/28 slots and 12× 50GE/25GE/10GE SFP56/28 slots, 2 × 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, 2× 1.92TB Storage and 4 AC power supplies.
FortiGate 4801F-DC	FG-4801F-DC	8× 400GE/200GE QSFP-DD slots, 12× 200GE/100GE/40GE QSFP56/28 slots and 12× 50GE/25GE/10GE SFP56/28 slots, 2 × 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, 2× 1.92TB Storage and 4x DC power supplies.
FortiGate 4801F-NEBS	FG-4801F-NEBS	8× 400GE/200GE QSFP-DD slots, 12× 200GE/100GE/40GE QSFP56/28 slots and 12x 50GE/25GE/10GE SFP56/28 slots, 2 × 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, 2× 1.92TB Storage and 4x AC power supplies, NEBS Level 3 compliant.
FortiGate 4801F-DC-NEBS	FG-4801F-DC-NEBS	8× 400GE/200GE QSFP-DD slots, 12× 200GE/100GE/40GE QSFP56/28 slots and 12× 50GE/25GE/10GE SFP56/28 slots, 2 × 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, 2× 1.92TB Storage and 4x DC power supplies.
Hyperscale Firewall License	LIC-FGT-HYPSC	Hyperscale Firewall License for FortiGate FG-4000F Series for hardware session setup acceleration and logging.
Optional Accessories/Spares	**SKU**	**Description**
Rack Mount Sliding Rails	SP-FG4K6K-RAIL	Rack mount sliding rails for FG-4200F, FG-4400F, FG-4800F, and FG-6000F.
AC Power Supply	SP-FG4000F-PS	2000W AC power supply for 4000F and 6000F series, does not include SP-FGPCORC15-XX power cord.
AC Power Cord	SP-FGPCORC15-XX	6 ft power cord, 15A125V XXX, PSE BLACK ROHS-6, for FG-3900E, 4000F, 6000F, and 7000E/F Series.
DC Power Supply	SP-FG4000F-DC-PS	DC power supply for FG-4200F-DC/4201F-DC, FG-4400F-DC/4401F-DC, FG-4800F-DC/4801F-DC and FG-6000F-DC, comes with 3m DC cable.
Fan Tray	SP-FG4K6K-FAN	Spare Hotswappable Fan Module for FG-420xF/440xF/480xF/6000F.

Ordering Information

Transceiver Modules	SKU	Description
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
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.
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 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 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all 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 all systems with SFP28 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.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short 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, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots.
100 GE QSFP28 Transceiver Module	FN-TRAN-QSFP28-DR	100 GE QSFP28 transceiver module, single channel single-mode fiber, 100GBase-DR 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 all systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, Short Range	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, 100m Range	FG-TRAN-QSFP28-SR4	100 GE QSFP28 transceiver module, 100m range, MMF, for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, CWDM4	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, Long Range 10km	FN-TRAN-QSFP28-LR1	100 GE QSFP28 transceiver module, long range 10km, LC connector, SMF, 1310nm, 100GBase-LR1, 0°C to 70°C, for systems with QSFP28 slots.
200 GE QSFP56 Transceiver Module, 2km Range	FN-TRAN-QSFP56-FR4	200 GE QSFP56 transceiver module, 2km range, SMF, for systems with QSFP56 slots.
400 GE QSFPDD Transceiver Module, 10km range	FN-TRAN-QSFPDD-LR4	400 GE QSFPDD transceiver module, 10km range, SMF, for systems with QSFP-DD slots.
400 GE QSFPDD Transceiver Module, 2km range	FN-TRAN-QSFPDD-FR4	400 GE QSFPDD transceiver module, 2km range, SMF, for systems with QSFP-DD slots.
400 GE QSFPDD Transceiver Module, 4 channel parallel fiber	FN-TRAN-QSFPDD-DR4	400 GE QSFPDD transceiver module, 4 channel parallel fiber, short range, for systems with QSFP-DD slots.
400 GE QSFPDD Transceiver Module, 8 channel parallel fiber	FN-TRAN-QSFPDD-SR8	400 GE QSFPDD transceiver module, 8 channel parallel fiber, short range, for systems with QSFP-DD slots.
Cables	**SKU**	**Description**
400 GE QSFPDD Passive Direct Attach Cable, 1m	FN-CABLE-QSFPDD-DAC-01	400 GE QSFPDD passive Direct Attach Cable, 1m, for systems with QSFP-DD slots.
400 GE QSFPDD Passive Direct Attach Cable, 2.5m	FN-CABLE-QSFPDD-DAC-B5	400 GE QSFPDD passive Direct Attach Cable, 2.5m, for systems with QSFP-DD slots.

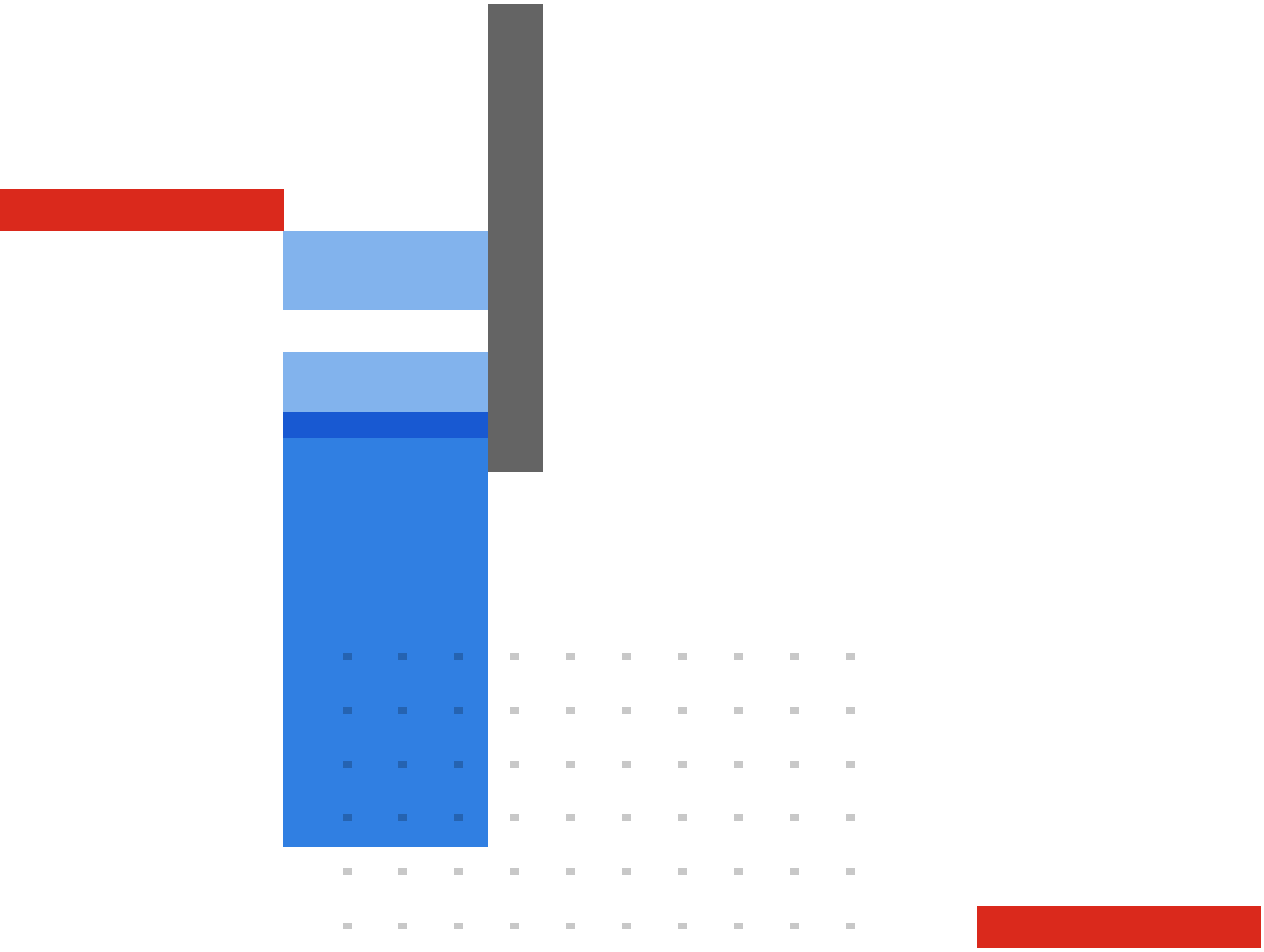
Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

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.

September 29, 2026

FG-4800F-DAT-R18-20260929