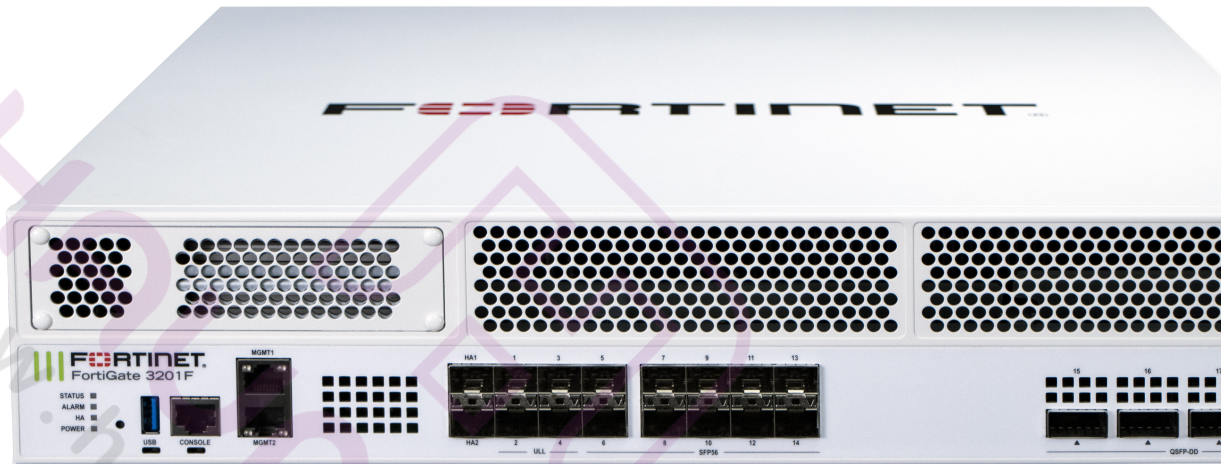


FortiGate 3200F Series

FG-3200F and 3201F



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and SD-WAN.

Security-Driven Networking FortiOS delivers converged networking and security.

Unparalleled Performance with Fortinet's patented / SPU / 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 3200F Series enables organizations to build security-driven networks that can weave security deep into their datacenter and across their hybrid IT architecture to protect any edge at any scale.

Powered by a rich set of AI/ML-based FortiGuard Services and an integrated security fabric platform, the FortiGate 3200F 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 3200F automatically controls, verifies, and facilitates user access to applications delivering consistent convergence with a seamless user experience.

IPS	NGFW	Threat Protection	Interfaces
63 Gbps	47 Gbps	45 Gbps	Multiple 400 GE QSFP-DD, 200GE QSFP56, 100 GE QSFP28, 50 GE SFP56, 40 GE QSFP+, 25 GE SFP28, 10 GE SFP+ slots, and 10 GE / GE RJ45 port



Available in



Appliance



Virtual



Hosted



Cloud



Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

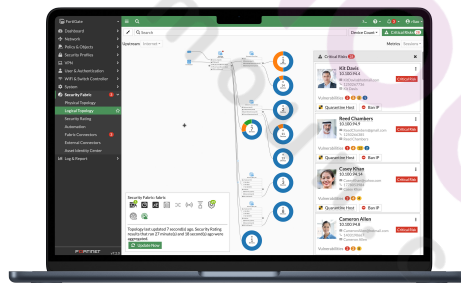
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

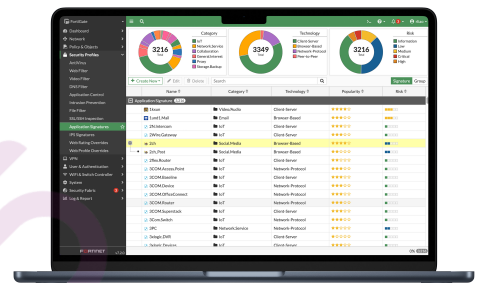
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations



Intuitive easy to use view into the network and endpoint vulnerabilities



Visibility with FOS Application Signatures

FortiConverter Service

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





FortiGuard Services

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

Zero-Day Threat Prevention

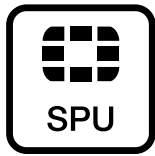
Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

OT Security

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



Secure Any Edge at Any Scale



Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

ASIC Advantage



Network Processor 7 NP7

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

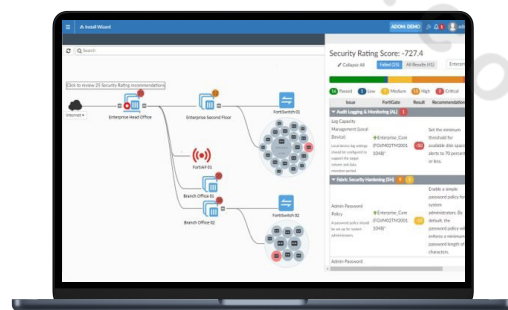
- Hyperscale firewall, accelerated session setup, and ultra-low latency
- Industry-leading performance for VPN, VXLAN termination, hardware logging, and elephant flows



Content Processor 9 CP9

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

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



Intuitive view and clear insights into network security posture with FortiManager

Centralized Network and Security Management at Scale

FortiManager, the centralized management solution from Fortinet, enables integrated management of the Fortinet security fabric, including devices like FortiGate, FortiSwitch, and FortiAP. It simplifies and automates the oversight of network and security functions across diverse environments, serving as the fundamental component for deploying Hybrid Mesh Firewalls.



Use Cases



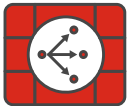
Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection



Segmentation

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



Secure SD-WAN

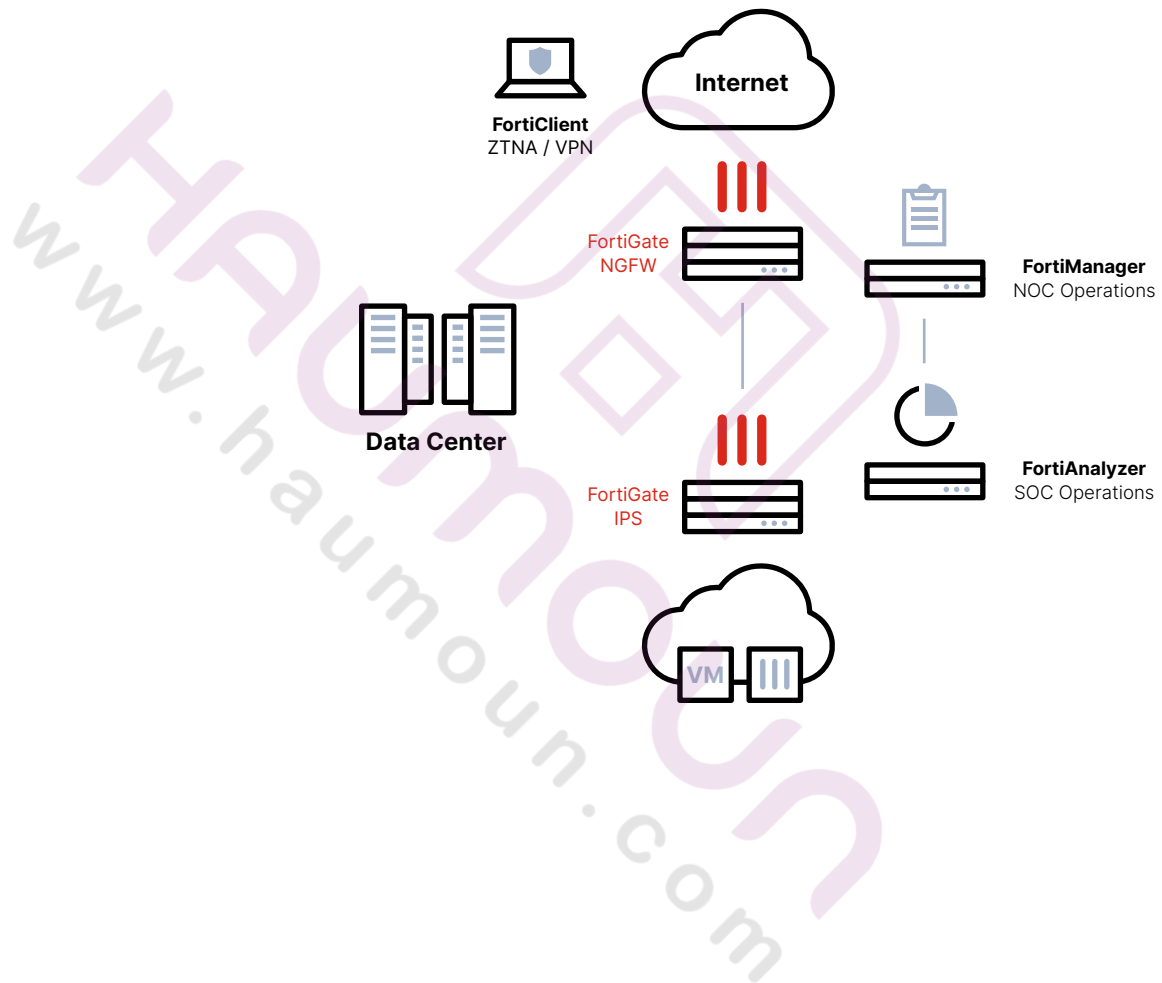
- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing



Mobile Security for 4G, 5G, and IoT

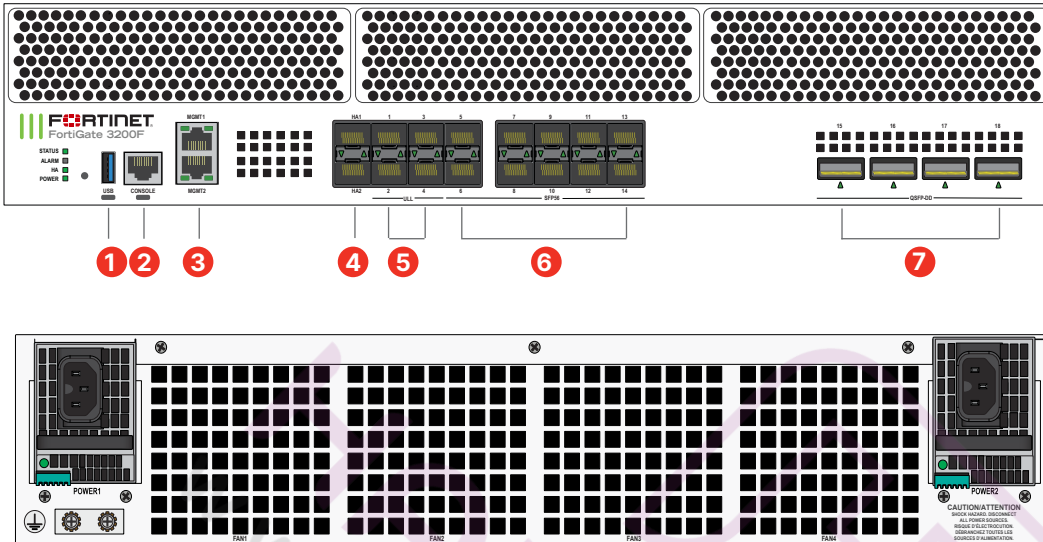
- SPU-accelerated, high performance CGNAT and IPv6 migration options, including: NAT44, NAT444, NAT64/ DNS64, NAT46 for 4G Gi/sGi, and 5G N6 connectivity and security
- RAN Access Security with highly scalable and highest-performing IPsec aggregation and control Security Gateway (SecGW)
- User plane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

Datacenter Deployment (NGFW, IPS, Segmentation)



Hardware

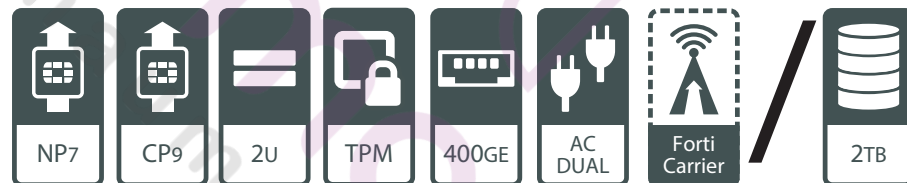
FortiGate 3200F Series



Interfaces

- 1 x USB Port
- 1 x RJ45 Console Port
- 2 × 10 GE / GE RJ45 Management Ports
- 2 × 50 GE SFP56 / 25 GE SFP28 / 10 GE SFP+ HA1/HA2 Slots
- 4 × 25 GE SFP28 / 10 GE SFP+ ULL Slots
- 10 × 50 GE SFP56 / 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots
- 4 × 400 GE QSFP-DD / 200 GE QSFP56 / 100 GE QSFP28 / 40 GE QSFP+ Slots

Hardware Features



Trusted Platform Module (TPM)

The FortiGate 3200F 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 3200F provides multiple 400GE/200GE QSFP-DD slots, simplifying network designs without relying on additional devices to bridge desired connectivity.

Specifications

	FG-3200F	FG-3201F
Interfaces and Modules		
Hardware Accelerated 400 GE QSFP-DD / 200 GE QSFP56 / 100 GE QSFP28 / 40 GE QSFP+ Ports		4
Hardware Accelerated 50 GE SFP56 / 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots		10
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP ULL Slots		4
Hardware Accelerated 50 GE SFP56 / 25 GE SFP28 / 10 GE SFP+ HA1/HA2 Slots		2
10 GE / GE RJ45 Management Ports		2
USB 3.0 Port		1
Console RJ45 Port		1
Onboard Storage		2 × 1 TB SSD
Trusted Platform Module (TPM)		Yes
Included Transceivers		2x SFP+ (SR 10 GE)
System Performance — Enterprise Traffic Mix		
IPS Throughput ²		63 Gbps
NGFW Throughput ^{2,4}		47 Gbps
Threat Protection Throughput ^{2,5}		45 Gbps
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)		387/385/178.5 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)		387/385/178.5 Gbps
Firewall Latency (64 byte, UDP)		3.42 μs / 1.45 μs*
Firewall Throughput (Packet per Second)		267.75 Mpps
Concurrent Sessions (TCP)		70 Million
New Sessions/Second (TCP)		800 000
Firewall Policies		200 000
IPsec VPN Throughput (512 byte) ¹		105 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		40 000
Client-to-Gateway IPsec VPN Tunnels		200 000
SSL-VPN Throughput		11 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		30 000
SSL Inspection Throughput (IPS, avg HTTPS) ³		29 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) ³		30 000
SSL Inspection Concurrent Session (IPS, avg HTTPS) ³		7.4 Million
Application Control Throughput (HTTP 64K) ²		109 Gbps
CAPWAP Throughput (HTTP 64K)		65 Gbps
Virtual Domains (Default / Maximum)		10 / 500
Maximum Number of FortiSwitches Supported		300
Maximum Number of FortiAPs (Total / Tunnel)		4096 / 2048
Maximum Number of FortiTokens		20 000
Maximum Number of Registered FortiClients		20 000

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.

	FG-3200F	FG-3201F
High Availability Configurations	Active-Active, Active-Passive, Clustering	
Dimensions and Power		
Height x Width x Length (inches)	3.5 × 17.44 × 23.9	
Height x Width x Length (mm)	88.9 × 443 × 607.1	
Weight	43.9 lbs (20 kg)	45.5 lbs (20.7 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2RU	
AC Power Supply	100–240VAC, 60/50 Hz	
Power Consumption (Average / Maximum)	520W / 865 W	527 W / 870 W
Current (Maximum)	12@100V, 9A@240V	
Heat Dissipation	2955 BTU/h	2971 BTU/h
Redundant Power Supplies (Hot Swappable)	Yes (Default dual AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80Plus Compliant	
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	71 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	

* Latency based on Ultra Low Latency (ULL) ports.



Ordering Information

Product	SKU	Description
Appliances		
FortiGate 3200F	FG-3200F	4x 400 GE QSFP-DD slots, 4x ULL SFP28 ports, and 12x 50 GE SFP56 slots (including 10x ports, 2x HA ports), 2x 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, and 2 AC power supplies.
FortiGate 3201F	FG-3201F	4x 400 GE QSFP-DD slots, 4x ULL SFP28 ports, and 12x 50 GE SFP56 slots (including 10x ports, 2x HA ports), 2x 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, 2 TB SSD onboard storage, and 2 AC power supplies.
Optional Accessories/Spares		
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1100/1101E, FG-1200D, FG-1500D/-DC, FG-1800F, FG-2000E, FG-2500E, FG-2600F, FG-2601F, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC, FG-3950B/-DC, FG-3200F, and FG-3201F
Spare Power Supply	SP-FG3800D-PS	AC power supply for FG-2200/2201E, FG-3000/3001F, FG-3200/3201F, FG-3300/3301E, FG-3400/3401E, FG-3500/3501F, FG-3600/3601E, FG-3700D, FG-3700D-NEBS, FG-3700DX, FG-3810D and FG-3815D, power cable SP-FGPCORHE-XX sold separately
Transceiver Modules		
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 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, (connects to FN-TRAN-SFP+BD27, ordered separately)	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 SFP28 transceiver module, short range for systems with SFP28 slots.
25 GE SFP28 Transceiver Module, Long Range	FN-TRAN-SFP28-LR	25 GE SFP28 transceiver module, long range for systems with SFP28 slots.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short range for systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Short Range BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceiver module, short range BiDi for systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, long range for systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module	FN-TRAN-QSFP+ER	40 GE QSFP+ transceiver module, 40km extended range for systems with QSFP+/QSFP28 slots.
50 GE SFP56 Transceiver Module, short range for systems with SFP56 slots.	FN-TRAN-SFP56-SR	50 GE SFP56 transceiver module, short range for systems with SFP56 slots.
100 GE QSFP28 Transceiver Module, Short Range	FN-TRAN-QSFP28-SR	100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, Long Range	FN-TRAN-QSFP28-LR	100 GE QSFP28 transceivers, 4 channel parallel fiber, long range for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, CWDM4	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for systems with QSFP28 slots.
100 GE QSFP28 BiDi Transceiver Module	FN-TRAN-QSFP28-BIDI	100 GE QSFP28 BiDi transceiver module, 100m MMF LC connector, for systems with QSFP28 slots.
100GE QSFP28 Transceiver Module	FN-TRAN-QSFP28-DR	100GE QSFP28 transceiver module, single channel single-mode fiber, 100GBase-DR for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, extended long range	FN-TRAN-QSFP28-ER	100GE QSFP28 transceiver module, extended long range 20km for systems with QSFP28 slots.
100 GE QSFP28 Transceiver Module, 100m Range	FN-TRAN-QSFP28-SR4	100 GE QSFP28 transceiver module, 100m range, MMF, for systems with QSFP28 slots.
200 GE QSFP56 Transceiver Module, 2km range	FN-TRAN-QSFP56-FR4	200 GE QSFP56 transceiver module, 2km range, for systems with QSFP56 slots.
200 GE QSFP56 Transceiver Module, short range, for systems with QSFP56 slots.	FN-TRAN-QSFP56-SR4	200 GE QSFP56 transceiver module, short range, 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, 2km Range	FN-TRAN-QSFPDD-DR4+	400 GE QSFPDD transceiver module, 4-channel parallel fiber, 2km range, for systems with QSFPDD 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.



Ordering Information

Product	SKU	Description
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.
50 GE SFP56 Passive Direct Attach Cable, 1m	FN-CABLE-SFP56-DAC-L1	50 GE SFP56 passive Direct Attach Cable, 1m 50 GE SFP56 passive Direct Attach Cable, 1m, for systems with SFP56 slots.
50 GE SFP56 Passive Direct Attach Cable, 2.5m	FN-CABLE-SFP56-DAC-LB5	50 GE SFP56 passive Direct Attach Cable, 2.5m 50 GE SFP56 passive Direct Attach Cable, 2.5m, for systems with SFP56 slots.
100 GE QSFP28 Passive Direct Attach Cable, 1m Range	FN-CABLE-QSFP28-1	100 GE QSFP28 passive direct attach cable, 1m range, for systems with QSFP28 slots.
200 GE QSFP56 Passive Direct Attach Cable, 1m	FN-CABLE-QSFP56-DAC-L1	200 GE QSFP56 passive Direct Attach Cable, 1m 200 GE QSFP56 passive Direct Attach Cable, 1m, for systems with QSFP56 slots.
200 GE QSFP56 Passive Direct Attach Cable, 2.5m	FN-CABLE-QSFP56-DAC-LB5	200 GE QSFP56 passive Direct Attach Cable, 2.5m 200 GE QSFP56 passive Direct Attach Cable, 2.5m, for systems with QSFP56 slots.
400 GE QSFPDD Active Optical Cable, 3m Range	FN-CABLE-QSFPDD-AOC-03	400 GE QSFPDD Active Optical Cable, 3m range, for systems with QSFP-DD slots.
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.



Subscriptions

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

1. Full features available when running FortiOS 7.4.1.

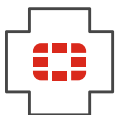
2. Desktop Models only.

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



FortiGuard Bundles

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.



FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive lifecycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service variants, offers heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an Extended End-of-Engineering-Support of 18 months, providing flexibility. Access the intuitive FortiCare Elite Portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.



Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, 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.