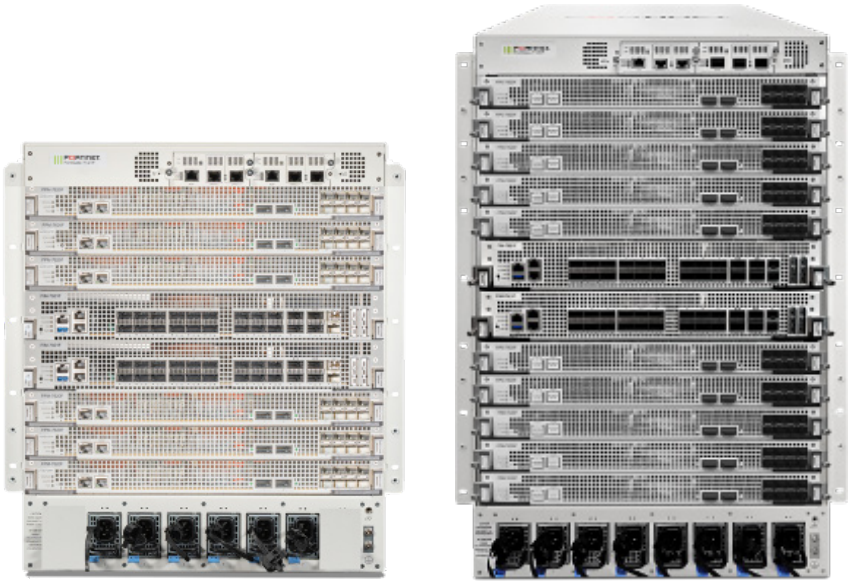
FortiGate 7000F Series



Highlights

Gartner® Magic Quadrant™ Leaders for both Network Firewalls and SD-WAN

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 7000F 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 7000F 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 7000F 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 7000F 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
FG-7081F	405 Gbps	330 Gbps	312 Gbps	25 GE SFP28 / 10 GE SFP+ / GE SFP 100 GE QSFP28 / 40 GE QSFP+ 400 GE QSFP-DD
FG-7121F	675 Gbps	550 Gbps	520 Gbps	

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

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. Infused with the latest threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero-day and sophisticated AI-powered attacks.

Network and file security

Network and file security services protect against network and file-based threats. With over 18,000 signatures, our industry-leading intrusion prevention system (IPS) uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, and applying virtual patches for newly discovered vulnerabilities. Anti-malware protection defends against both known and unknown file-based threats, combining antivirus and sandboxing for multi-layered security. Application control improves security compliance and provides real-time visibility into applications and usage.

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 over 300 million URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks. FortiGuard Labs blocks over 500 million malicious/phishing/spam URLs weekly, and blocks 32,000 botnet command-and-control attempts every minute, demonstrating the robust protection offered through Fortinet.

SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This includes data loss prevention to ensure visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. Our inline cloud access security broker service protects data in motion, at rest, and in the cloud, enforcing compliance standards and managing account, user, and cloud app usage. Services also assess infrastructure, validate configurations, and highlight risks and vulnerabilities, including IoT device detection and vulnerability correlation.

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 malware in real time, delivering sub-second protection across all NGFWs. The service also integrates the MITRE ATT&CK matrix to speed up investigations. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

OT security

With over 1000 virtual patches, 1100+ OT applications, and 3300+ 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.

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

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

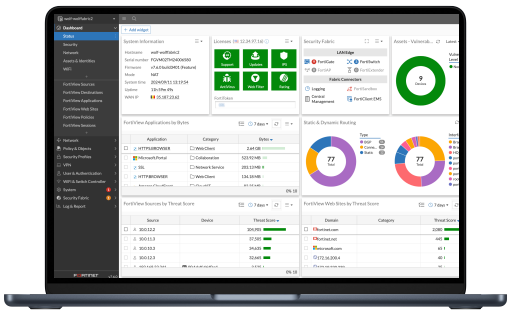
FortiOS is the operating system that powers Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. FortiOS provides a unified framework for managing and securing networks, cloud-based, hybrid, or a convergence of IT, OT, and IoT. FortiOS enables seamless and efficient interoperation across Fortinet products with consistent and consolidated AI-powered protection across today's hybrid environments.

Unlike traditional point solutions, Fortinet adopts a holistic approach to cybersecurity, aiming to reduce complexities, eliminate security silos, and improve operational efficiencies. By consolidating security functions into a single platform, FortiOS simplifies management, reduces costs, and enhances overall security posture. Together, FortiGate and FortiOS create intelligent, adaptive protection to help organizations reduce complexity, eliminate security silos, and optimize user experience.

By integrating generative AI (GenAI), FortiOS further enhances the ability to analyze network traffic and threat intelligence, detects deviations or anomalies more effectively, and provides more precise remediation recommendations, ensuring minimum performance impact without compromising security.

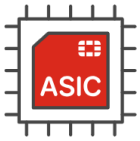
Learn more about what's new in FortiOS. https://www.fortinet.com/products/fortigate/fortios

Intuitive easy to use view into the network and endpoint vulnerabilities



Comprehensive view of network performance, security, and system status

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

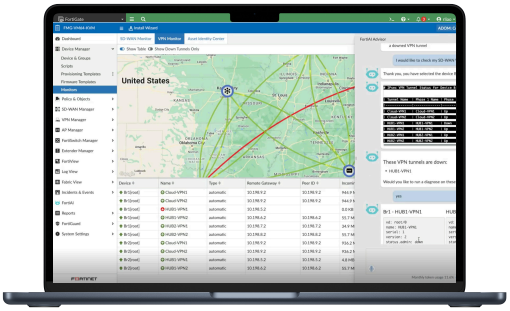
Content processors act as co-processors to offload resource-intensive processing of security functions. The ninth generation of the Fortinet Content Processor, the CP9, accelerates resource-intensive SSL (including TLS 1.3) decryption and security functions while delivering:

- 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

FortiManager

Centralized management at scale for distributed enterprises

FortiManager, powered by FortiAI, is a centralized management solution for the Fortinet Security Fabric. It streamlines mass provisioning and policy management for FortiGate, FortiGate VM, cloud security, SD-WAN, SD-Branch, FortiSASE, and ZTNA in hybrid environments. Additionally, FortiManager provides real-time monitoring of the entire managed infrastructure and automates network operation workflows. Leveraging GenAI in FortiAI, it further enhances Day 0–1 configurations and provisioning, and Day N troubleshooting and maintenance, unlocking the full potential of the Fortinet Security Fabric and significantly boosting operational efficiency.



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.

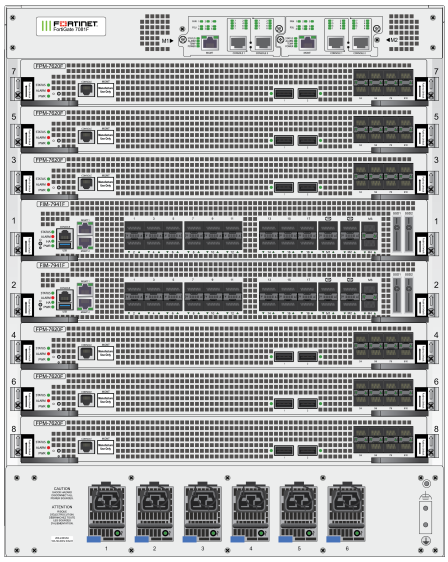
FortiCare Services

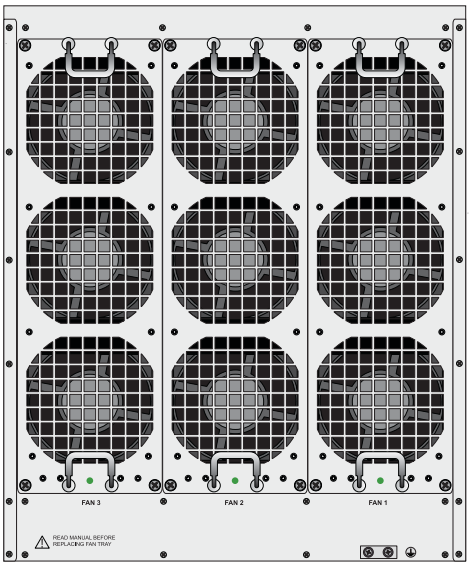
Expertise at your service

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.

Hardware

FortiGate 7081F Series





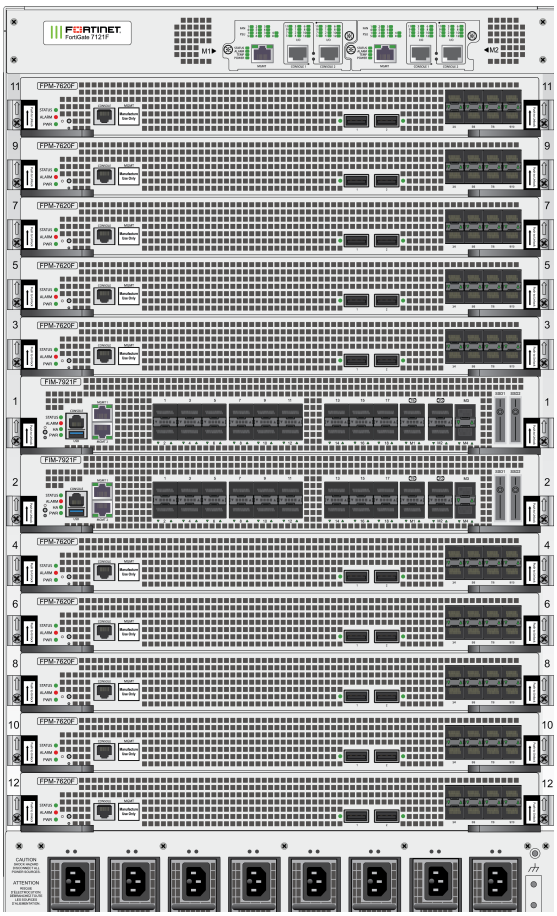
	FG-7081F/ FG-7081F-DC	FG-7081F-2/ FG-7081F-2-DC
Hardware Interfaces		
Hardware Accelerated 400 GE QSFP-DD / 100 GE QSFP28 / 40 GE QSFP+ Slots	16	
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots	36	
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+	48	
Management/HA Slots	4	
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ Slots	80	
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ SFP Management/HA Slots	4	
USB Ports	2	
Console Ports	8	
Onboard Storage	4× 4 TB SSD	
Included Transceivers	4× 10 GE SFP+ SR	
Trusted Platform Module (TPM)	✓	
Bluetooth Low Energy (BLE)	—	
Signed Firmware Hardware Switch	—	
System Performance and Capacity*		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP packets)	1.89 / 1.88 / 1.129 Tbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP packets)	1.89 / 1.88 / 1.129 Tbps	
Firewall Latency (64 byte, UDP)	7.5 µs	
Firewall Throughput (Packet per Second)	1680 Mpps	
Concurrent Sessions (TCP)	600 Million	
New Sessions/Sec (TCP)	5.4 Million	
Firewall Policies	200 000	
IPsec VPN Throughput (512 byte) [6]	378 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	40 000	
Client-to-Gateway IPsec VPN Tunnels	260 000	
SSL-VPN Throughput [7]	13.5 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30 000	

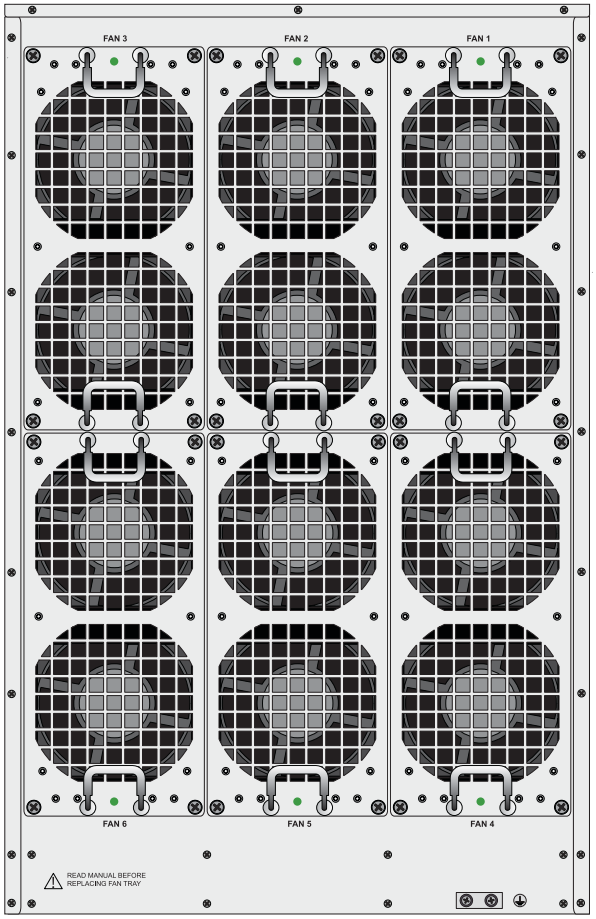
	FG-7081F/ FG-7081F-DC	FG-7081F-2/ FG-7081F-2-DC
IPS Throughput (Enterprise Mix) [1]	405 Gbps	
SSL Inspection Throughput [2]	324 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	288 000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	60 M	
Application Control Throughput (HTTP 64K) [3]	900 Gbps	
NGFW Throughput [4]	330 Gbps	
Threat Protection Throughput [2,5]	312 Gbps	
CAPWAP Throughput	N/A	
Virtual Domains (Default / Maximum)	10/500	
Maximum Number of FortiTokens	12 000	
Maximum Number of FortiSwitches Supported	300	
Maximum Number of FortiAPs (Total / Tunnel Mode)	N/A	
High Availability Configurations	Active-Active (FGSP), Active-Passive, Clustering	
Dimensions and Power		
Height x Width x Length (inches)	21.41 × 17.33 × 26.6	
Height x Width x Length (mm)	543.9 × 440 × 675.5	
Weight	165.68 kg / 365.26 lbs	
AC Power Supply	200 to 277 VAC (50/60 Hz)	
DC Power Supply	-48V to -60V DC	
Power Consumption (Average / Maximum)	6100 W / 7300 W	6160 W / 7370 W
AC Current (Maximum)	16A x 6	
DC Current (Average/Maximum)	127@48V / 152A@48V	128@48V / 154A@48V
Heat Dissipation (Average)	24 900 BTU/h	25 174 BTU/h
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	
Compliance		
Certifications	TBA	

* Performance specifications for FG-7081F/ 7081F-2 are based on 6 FPM combination.

Hardware

FortiGate 7121F





Trusted Platform Module (TPM)

The FortiGate 7000F 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.

Specifications

	FG-7121F*	FG-7121F-DC FG-7121F-2-DC
Interfaces and Modules		
Hardware Accelerated 400 GE QSFP-DD / 100 GE QSFP28 / 40 GE QSFP+ Slots	24	
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots	36	
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Management/HA Slots	4	
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ Slots	80	
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ SFP Management/HA Slots	4	
GE RJ45 Management Ports	4	
USB Ports	2	
Console Ports	14	
Trusted Platform Module (TPM)	✓	
Bluetooth Low Energy (BLE)	—	
Signed Firmware Hardware Switch	—	
Onboard Storage	4× 4 TB SSD	
Included Transceivers	4× 10 GE SFP+ SR	
System Performance - Enterprise Traffic Mix		
IPS Throughput [2]	675 Gbps	
NGFW Throughput [2, 4]	550 Gbps	
Threat Protection Throughput [2, 5]	520 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518/512/64 byte, UDP packets)	1.89 / 1.88 / 1.129 Tbps	
IPv6 Firewall Throughput (1518/512/86 byte, UDP packets)	1.89 / 1.88 / 1.129 Tbps	
Firewall Latency (64 byte, UDP)	7.50 µs	
Firewall Throughput (Packet per Second)	1680 Mpps	
Concurrent Sessions (TCP)	1 Billion	
New Sessions/Sec (TCP)	9 Million	
Firewall Policies	200 000	
IPsec VPN Throughput (512 byte) [6]	630 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	40 000	
Client-to-Gateway IPsec VPN Tunnels	260 000	
SSL-VPN Throughput [7]	13.7 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum)	30 000	
IPS Throughput (Enterprise Mix)[1]	675 Gbps	
SSL Inspection Throughput[3]	540 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	480 000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	100 Million	
Application Control Throughput (HTTP 64K) [3]	1.5 Tbps	
NGFW Throughput [4]	550 Gbps	
Threat Protection Throughput [2,5]	520 Gbps	
CAPWAP Throughput	N.A.	

	FG-7121F*	FG-7121F-DC FG-7121F-2-DC
Virtual Domains (Default / Maximum)	10 / 500	
Maximum Number of FortiTokens	20 000	
Maximum Number of FortiSwitches Supported	300	
Maximum Number of FortiAPs (Total / Tunnel Mode)	N.A.	
High Availability Configurations	Active-Active (FGSP), Active-Passive, Clustering	
Dimensions and Power		
Height x Width x Length (inches)	28.63 × 17.33 × 26.6	
Height x Width x Length (mm)	727.2 × 440 × 675.5	
Weight (maximum)	447.36 lbs (203.1 kg)	
Form Factor (supports EIA/non-EIA standards)	16 RU 10 Slots for FPM and 2 Slots for FIM (default configuration 2xFPM-7620F and 2xFIM-7921F)	
Power Required	200 to 277 VAC (50/60 Hz)	
Power Consumption (Maximum / Average)	9754 W / 8296 W	9754W / 8296W 9820W / 8356W
AC Current (Maximum)	8 × 10A	
DC Current (Average/Maximum)		17A@48V/ 204A@48V 174@48V / 205A@48V
Heat Dissipation (Maximum)	33 261 BTU/h	
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	
Compliance		
Certifications	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	

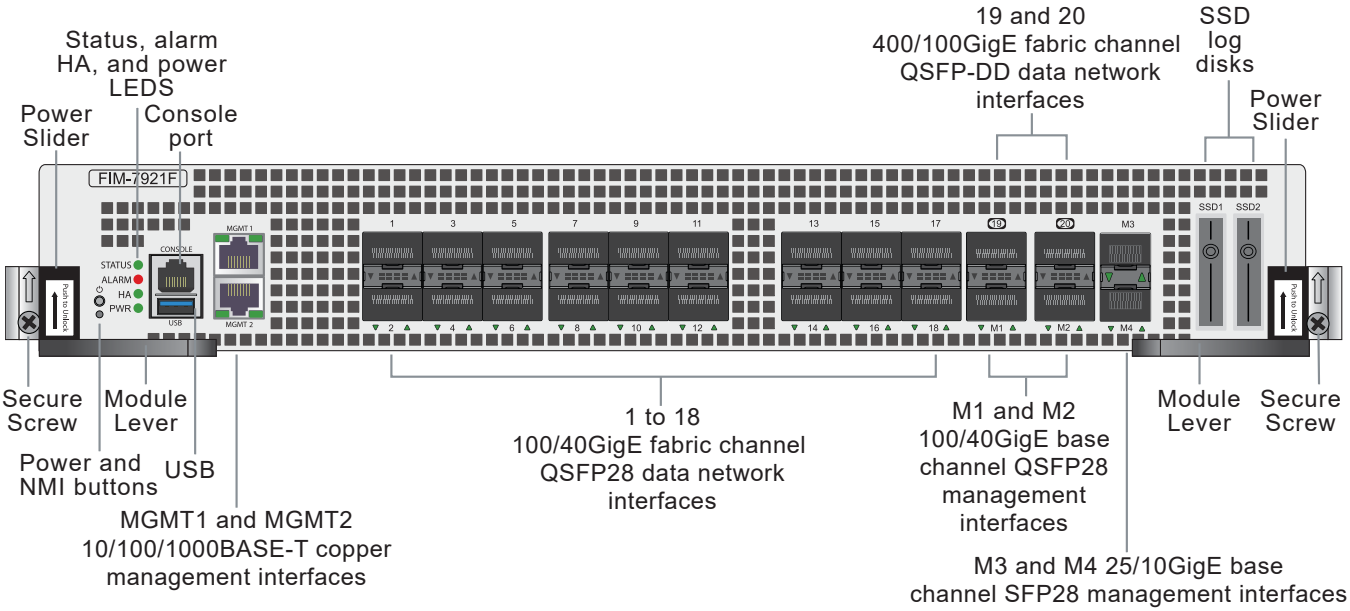
* Performance specifications for FG-7121F are based on 10 FPM combination.

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 with sandboxing enabled.
6. Measured with VPN load balancing.
7. Measured on single FPM only.

Hardware

Fortinet Interface Module FIM-7921F and FIM-7941F



Hardware Features

NP7 | TPM | 400/100/40/25/10/GE | 8TB

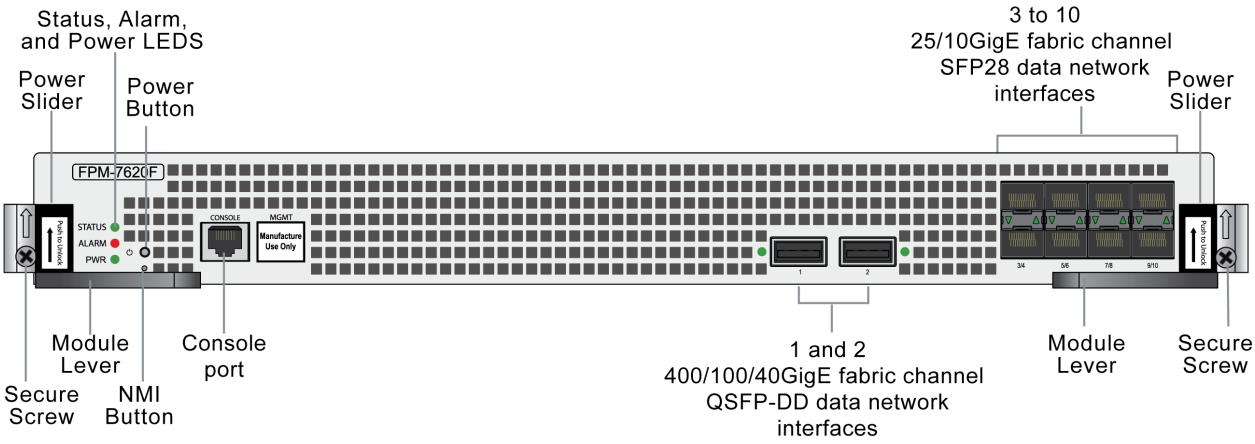
Specifications

	FIM-7921F	FIM-7941F
Hardware Interfaces		
Hardware Accelerated 400 GE QSFP-DD / 100 GE QSFP28 / 40 GE QSFP+ Slots	2[1]	2[1]
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots	18[2]	18[3]
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Management/HA Slots	2	2
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ SFP Management/HA Slots	2	2
GE RJ45 Management Ports	2	2
USB Ports	1	1
Console Ports	1	1
Trusted Platform Module (TPM)	✓	✓
Bluetooth Low Energy (BLE)	—	—
Signed Firmware Hardware Switch	—	—
Onboard Storage	2 × 4 TB SSD	2 × 4 TB SSD
Included Transceivers	2 × 10 GE SFP+ SR	2 × 10 GE SFP+ SR
Dimensions and Power		
Height x Width x Length (inches)	2.48 × 17.11 × 18.56	2.48 × 17.11 × 18.56
Height x Width x Length (mm)	63 × 435 × 471.3	63 × 435 × 471.3
Weight	21.48 lbs (9.75 kg)	25.66 lbs (11.65 kg)
Power Consumption (Average / Maximum)	568 W / 597 W	598 W / 630 W
Current (Maximum)	50A	53A
Heat Dissipation (Average)	2036 BTU/h	2149 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	-31°F to 158°F (-35°C to 70°C)
Humidity	5% to 90% non-condensing	5% to 90% non-condensing
Compliance		
Certifications	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	

1. Ports 19 and 20 can be configured as split ports
2. Ports 1-8 can be configured as split ports
3. Ports 1-18 can be configured as split ports

Hardware

Fortinet Processor Module FPM-7620F



Specifications

	FPM-7620F
Hardware Interfaces	
Hardware Accelerated 400 GE QSFP-DD / 100 GE QSFP28 / 40 GE QSFP+ Slots	2
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ Slots	8
Console Port	1
Trusted Platform Module (TPM)	✓
Bluetooth Low Energy (BLE)	—
Signed Firmware Hardware Switch	—
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP packets)	396 / 395 / 263 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP packets)	396 / 395 / 263 Gbps
Firewall Latency (64 byte, UDP)	7.50 µs
Firewall Throughput (Packet per Second)	39 286 Mpps
Concurrent Sessions (TCP)	100 Million
New Sessions/Sec (TCP)	900K
Firewall Policies	200 000 (system wide)
IPsec VPN Throughput (512 byte) [6]	63 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	4000
Client-to-Gateway IPsec VPN Tunnels	26 000
SSL-VPN Throughput [7]	13.7 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	30 000
IPS Throughput (Enterprise Mix) [1]	67.5 Gbps
SSL Inspection Throughput [2]	54 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	48 000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	10 Million

Hardware Features

■ NP7 ■ CP9 ■ TPM ● 100/40/25/10/GE

	FPM-7620F
Application Control Throughput (HTTP 64K) [3]	150 Gbps
NGFW Throughput [4]	55 Gbps
Threat Protection Throughput [5]	52 Gbps
CAPWAP Throughput	N.A.
Virtual Domains (Default / Maximum)	10 / 500
Maximum Number of FortiTokens	2000
Maximum Number of FortiSwitches Supported	300
Maximum Number of FortiAPs (Total / Tunnel Mode)	N.A.
High Availability Configurations	Active-Passive, Active-Active
Dimensions and Power	
Height x Width x Length (inches)	1.69 × 17.11 × 18.56
Height x Width x Length (mm)	43 × 435 × 471
Weight	16.19 lb. (7.35 kg)
Power Consumption (Average / Maximum)	675 W / 716 W
Current (Maximum)	60A
Heat Dissipation (Average)	2442 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)
Storage Temperature	-13°F to 158°F (-25°C to 70°C)
Humidity	5% to 90% non-condensing
Compliance	
Certifications	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB

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 with sandboxing enabled.
6. Measured with VPN load balancing.
7. Measured on single FPM only.

Subscriptions

			Bundles		
Service Category	Service Offering	A-la-carte	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct [3], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video [3] Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention [3]	•	•		
	Data Loss Prevention (DLP) [1]	•	•		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	•	•		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS [1]	•			
	Application Control		----------included with FortiCare Subscription----------		
	Inline CASB [3]		----------included with FortiCare Subscription----------		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring	Models up to FG/FWF-60F series			
	SD-WAN Underlay and Application Monitoring Service	FG-70F series and above			
	SD-WAN Overlay-as-a-Service	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	SASE expansion for SD-WAN (SD-WAN SPA Connector license plus FortiSASE starter kit for n* users) [2]	Selected models only[2]			
	SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth)	Desktop models only			
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. Full features available when running FortiOS 7.4.1.

2. See the FortiSASE Ordering Guide for supported models and their associated number of user licenses.

3. 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.

FortiGuard Bundles

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 Model		
FortiGate 7081F	FG-7081F	12U 8-slot chassis starting with 1x FPM-7620F Processor Module, 1x FIM-7921F I/O Module, 2x Management Module and 6x hot swappable redundant PSU (2500WAC).
FortiGate 7081F-DC	FG-7081F-DC	12U 8-slot chassis starting with 1x FPM-7620F Processor Module, 1x FIM-7921F I/O Module, 2x Management Module and 6x hot swappable redundant PSU (2500WDC).
FortiGate 7081F-2	FG-7081F-2	12U 8-slot chassis starting with 1x FPM-7620F Processor Module, 1x FIM-7941F I/O Module, 2x Management Module and 6x hot swappable redundant PSU (2500WAC).
FortiGate 7081F-2-DC	FG-7081F-2-DC	12U 8-slot chassis starting with 1x FPM-7620F Processor Module, 1x FIM-7941F I/O Module, 2x Management Module and 6x hot swappable redundant PSU (2500WDC).
FortiGate 7121F*	FG-7121F	16U 12-slot chassis with 2x FPM-7620F Processor Module, 2x FIM-7921F I/O Module, 2x Management Module and 8x hot swappable redundant PSU.
FortiGate-7121F-2	FG-7121F-2	16U 12-slot chassis with 2x FPM-7620F Processor Module, 2x FIM-7941F I/O Module, 2x Management Module and 8x hot swappable redundant PSU.
FortiGate-7121F-DC	FG-7121F-DC	16U 12-slot chassis with 2x FPM-7620F Processor Module, 2x FIM-7921F I/O Module, 2x Management Module and 8x hot swappable redundant PSU 2KW DC-DC (without DC combiner).
OPTIONAL / SPARE ITEMS	**SKU**	**DESCRIPTION**
Processor Module		
FPM-7620F Module	FPM-7620F	Hot swappable processing module for 7xxxF series - FortiASIC NP7 and CP9 hardware accelerated. 2x QSFP28 and 8x SFP28 ports.
I/O Module		
FIM-7921F Module**	FIM-7921F	Hot swappable I/O module for 7xxxF series - FortiASIC NP7 hardware accelerated. 2x GE RJ45 Management ports, 2x QSFP-DD ports, 20x QSFP28 ports, 2x SFP28 ports. 2× 4TB local log storage.
FIM-7941F Module**	FIM-7941F	Hot swappable I/O module for 7xxxF series - FortiASIC NP7 hardware accelerated. 2x GE RJ45 Management ports, 2x QSFP-DD ports, 20x QSFP28 ports, 2x SFP28 ports. 2× 4TB local log storage.
Accessories		
FortiGate 7121F Fan Module	FG-7121F-FAN	FG-7121F Fan module.
FortiGate 7121F Power Supply	FG-7121F-PS-2KAC	FG-7121F power supply 2KW AC.
FortiGate-7121F-AC-Chassis	FG-7121F-CH	FG-7121F chassis with 2x system management module, 8x PSU and 6x FAN module.
FortiGate-7121F-DC-Chassis	FG-7121F-DC-CH	FG-7121F chassis with 2x system management module, 8x DC PSU and 6x FAN module, 8x DC input cable.
FG-7121F-DC-Combiner	FG-7121F-DC-COMBINER	1U rack mounted chassis containing 8x DC combiner module to support A+B input redundancy for FG-7121F-DC.
FortiGate 7081F Chassis	FG-7081F-CH	FG-7081F chassis with 2x system management module, 6× 2500WAC PSU and 3x FG-7081F FAN module.
Fortigate-7000F 2500W DC Power Supply	FG7K-PS-2K5DC	Fortigate-7000F 2500W DC Power supply.
Fortigate-7000F 2500W AC Power Supply	FG7K-PS-2K5AC	Fortigate-7000F 2500W AC Power supply.
FortiGate 7081F Fan Module	FG-7081F-FAN	FG-7081F fan module.

Ordering Information

PRODUCT	SKU	DESCRIPTION
Transceivers		
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 Module (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+ Transceiver Module	FN-TRAN-SFP+ER	10 Gbase-ER SFP+ transceivers for FortiSwitch and FortiGate, 1550nm. Single Mode. 40km range for systems with SFP+ slots.
25 GE SFP28 Transceiver Module, short range	FN-TRAN-SFP28-SR	25 GE/10 GE 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.
40 GE QSFP+ Transceiver Module, short range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceivers, short range for all 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.
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, short range, 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, 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, SMF, for systems with QSFP56 slots.
200 GE QSFP56 Transceiver Module, 100m Range	FN-TRAN-QSFP56-SR4	200 GE QSFP56 transceiver module, 100m range, MMF, for systems with QSFP56 slots.
400 GE QSFP-DD Transceiver Module, 10km range	FN-TRAN-QSFPDD-LR4	400 GE QSFP-DD transceiver module, 10km range, SMF, for systems with QSFP-DD slots.
400 GE QSFP-DD Transceiver Module, 2km range	FN-TRAN-QSFPDD-FR4	400 GE QSFP-DD transceiver module, 2km range, SMF, for systems with QSFP-DD slots.
400 GE QSFP-DD Transceiver Module, 4 channel parallel fiber	FN-TRAN-QSFPDD-DR4	400 GE QSFP-DD transceiver module, 4 channel parallel fiber, short range, for systems with QSFP-DD slots.
400 GE QSFP-DD Transceiver Module, 8 channel parallel fiber	FN-TRAN-QSFPDD-SR8	400 GE QSFP-DD transceiver module, 8 channel parallel fiber, short range, for systems with QSFP-DD slots.
400 GE QSFP-DD Transceiver Module, 4 Channel Parallel Fiber, 2km Range	FN-TRAN-QSFPDD-DR4+	400 GE QSFP-DD transceiver module, 4 channel parallel fiber, 2km range, for systems with QSFP-DD slots.
Cables		
40 GE QSFP+ Passive Direct Attach Cable	SP-CABLE-FS-QSFP+5	40GE QSFP+ Passive Direct Attach Cable, 5m for Systems with QSFP+ 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.
400 GE QSFP-DD Passive Direct Attach Cable, 1m	FN-CABLE-QSFPDD-DAC-01	400 GE QSFP-DD passive Direct Attach Cable, 1m, for systems with QSFP-DD slots.
400 GE QSFP-DD Passive Direct Attach Cable, 2.5m	FN-CABLE-QSFPDD-DAC-B5	400 GE QSFP-DD passive Direct Attach Cable, 2.5m, for systems with QSFP-DD slots.
400 GE QSFP-DD Active Optical Cable, 3m Range	FN-CABLE-QSFPDD-AOC-03	400 GE QSFP-DD Active Optical Cable, 3m range, for systems with QSFP-DD slots.

* The FG-7081F and FG-7121F have Chassis-based pricing. Individual and bundled FortiGuard security services and FortiCare support subscription services such as Threat Protection Bundle, UTM Bundle, Enterprise Bundle, and FortiCare360 are on a chassis-based pricing. License such as VDOM and Endpoint Compliance are also included in the chassis-based pricing.

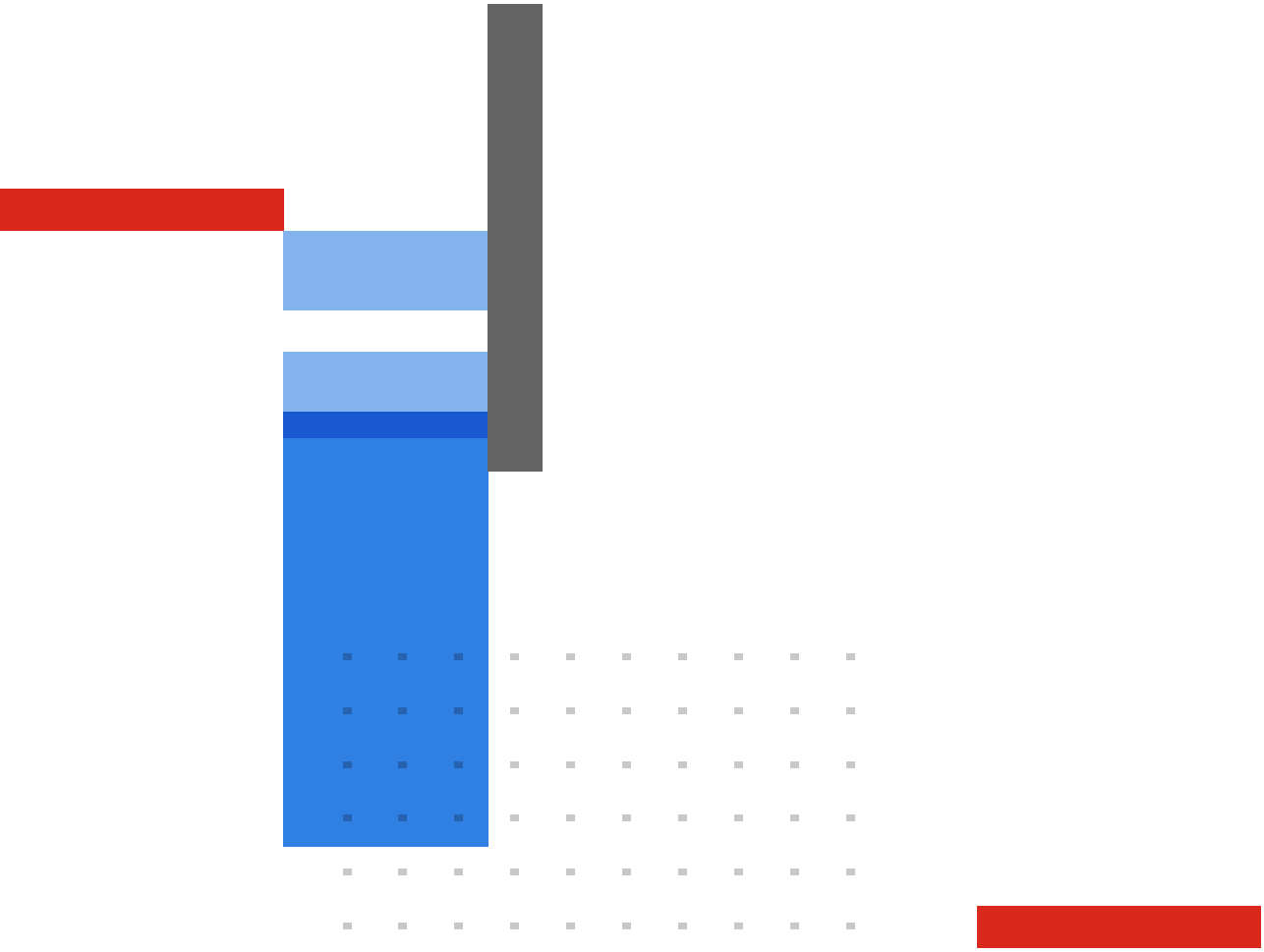
** Each FIM is packed individually and comes with 2× 10 GE SFP+ SR transceivers at no charge.

NOTE: All optional/spare components are for replacement usage and should not be used to assemble a bundle as only bundles have the necessary subscriptions.

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.



FORTINET

www.fortinet.com

April 7, 2025

FG-7000F-DAT-R18-20250407