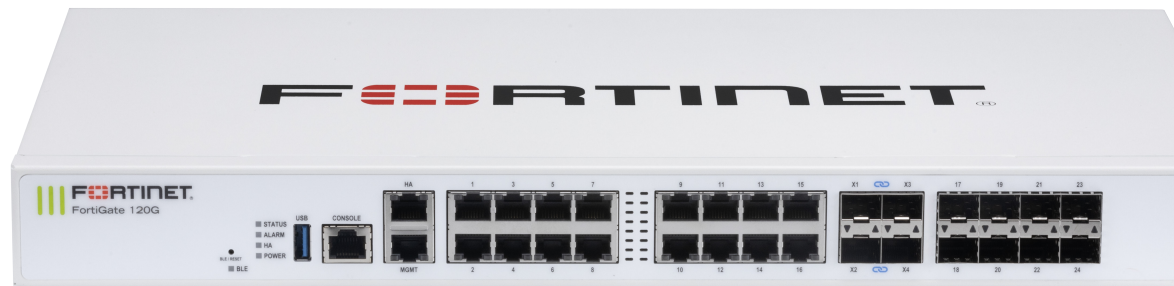


# FortiGate 120G Series



## Highlights

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

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

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

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

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

## Artificial Intelligence, Machine Learning Security with Deep Visibility

The FortiGate 120G series next-generation firewall (NGFW) combines artificial intelligence (AI)-powered security and machine learning (ML) to deliver threat protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 120G Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks. This security fabric seamlessly extends across your entire environment, including a Hybrid Mesh Firewall architecture, ensuring consistent policy enforcement and threat protection across all network segments.

Universal zero-trust network access (ZTNA) automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users. Ultra-fast threat protection and SSL inspection provides security at the edge you can see without impacting performance.

IPS	NGFW	Threat Protection	Interfaces
5.3 Gbps	3.1 Gbps	2.8 Gbps	Multiple GE RJ45, SFP, and 10GE SFP+ Slots Variants with internal storage

## Use Cases



### Next Generation Firewall (NGFW)

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



### Secure SD-WAN

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



### Universal ZTNA

- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD



Available in



Appliance



Virtual



Hosted



Cloud



Container

## FortiOS Everywhere

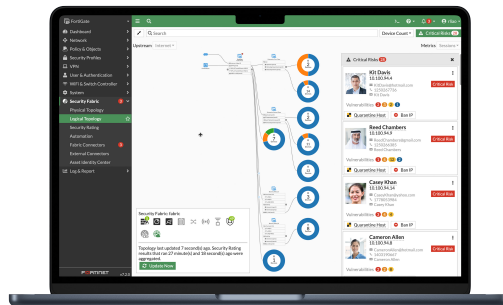
### FortiOS, Fortinet's Real-Time Quantum-Safe Network Security Operating System

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

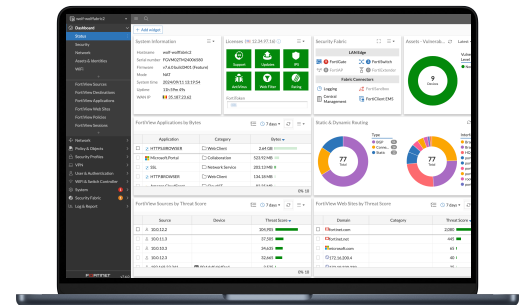
By converging networking and security functions into a single operating system, organizations can manage network and security more effectively to detect, investigate, and respond to incidents faster. This unified architecture simplifies operations, eliminates security silos, and allows organizations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

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

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



*Intuitive easy to use view into the network and endpoint vulnerabilities*



*Comprehensive view of network performance, security, and system status*





## FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Powered by real-time AI enhanced threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero days and evasive, sophisticated AI-powered attacks.

### Network and file security

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

### Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of millions of URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks.

### SaaS and data security

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

### Zero-Day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown and zero-day malware in real time, delivering sub-second protection across all NGFWs. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

### Attack surface visibility and compliance

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

### OT security

With over 2400 virtual patches, 1600+ OT applications, and 3500+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.



## FortiManager

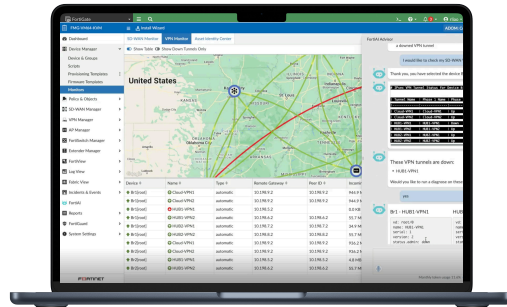
### AI-Powered, Automation-Driven, Enterprise-Class Centralized Management at Scale



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

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

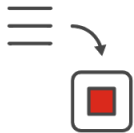
FortiManager integrates with FortiSOC for contextual insights and fabric-wise response. It also supports ecosystem integrations, and open APIs for extended automation. ADOM-based administration and FortiManager clusters enables resilient control across distributed networks.



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

## FortiConverter Service

### Migration to FortiGate NGFW made easy



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

## FortiCare Services

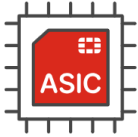
### Expertise at your service



Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an extended end-of-engineering support of 18 months, providing flexibility and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.



## Fortinet ASICs: Unrivaled Security, Unprecedented Performance



### Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

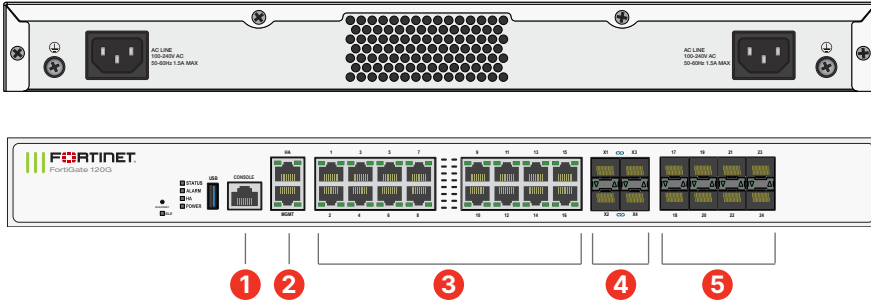
---

### Secure SD-WAN ASIC SP5

- Combines a RISC-based CPU with Fortinet's proprietary security processing unit (SPU) content and network processors for unmatched performance
- Delivers the industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for the best user experience on direct internet access
- Enables best-of-breed NGFW security and deep SSL inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

## Hardware

### FortiGate 120G/121G Series



### Interfaces

1. 1x RJ45 Console Port
2. 2x RJ45 HA and Management Ports
3. 16x GE RJ45 Ports
4. 4x 10GE SFP+ FortiLink Slots
5. 8x SFP Ports

### Hardware Features



#### Trusted Platform Module (TPM)

The FortiGate 120G series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.



#### Dual power supply

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 120G series offers dual built-in non-hot swappable power supplies.



#### Access layer security

FortiLink protocol enables you to converge security and network access by integrating the FortiSwitch into the FortiGate as a logical extension of the firewall. These FortiLink-enabled ports can be reconfigured as regular ports as needed.

## Specifications

	FORTIGATE 120G	FORTIGATE 121G
<b>Hardware Specifications</b>		
Hardware Accelerated GE RJ45 Ports		16
GE RJ45 Management / HA		1 / 1
Hardware Accelerated GE SFP Slots		8
Hardware Accelerated 10 GE SFP+ FortiLink Slots (default)		4
USB Ports		1
Console (RJ45) Port		1
Internal Storage	—	1 × 480 GB SSD
Trusted Platform Module (TPM)		☑
Bluetooth Low Energy (BLE)		☑
Signed Firmware Hardware Switch		—
<b>System Performance* — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		5.3 Gbps
NGFW Throughput <sup>2,4</sup>		3.1 Gbps
Threat Protection Throughput <sup>2,5</sup>		2.8 Gbps
<b>System Performance and Capacity</b>		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)		39 / 39 / 28 Gbps
Firewall Latency (64 byte UDP packets)		3.17 μs
Firewall Throughput (Packets Per Second)		42 Mpps
Concurrent Sessions (TCP)		3 M
New Sessions/Second (TCP)		140 000
Firewall Policies		10 000
IPsec VPN Throughput (512 byte) <sup>1</sup>		35 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		2000
Client-to-Gateway IPsec VPN Tunnels		16 000
SSL-VPN Throughput		1.5 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		500
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>		3 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>		2100
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>		315 000
Application Control Throughput (HTTP 64K) <sup>2</sup>		6.7 Gbps
CAPWAP Throughput (HTTP 64K)		35 Gbps
Virtual Domains (Default / Maximum)		10 / 10
Maximum Number of FortiSwitches Supported		48*
Maximum Number of FortiAPs (Total / Tunnel Mode)		128 / 64
Maximum Number of FortiTokens		5000
High Availability Configurations		Active-Active, Active-Passive, Clustering

	FORTIGATE 120G	FORTIGATE 121G
<b>Dimensions</b>		
Height x Width x Length (inches)	1.73 × 17 × 10	
Height x Width x Length (mm)	44 × 432 × 254	
Weight	12.17 lbs (5.52 kg)	
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 1RU	
<b>Operating Environment and Certifications</b>		
Input Rating	100-240VAC, 60-50Hz	
Power Supply Efficiency Rating	N/A	
Redundant Power Supplies	Yes (Default dual non-swappable AC PSU for 1+1 Redundancy)	
Maximum Current	1.0A @100V, 0.5A @240V	
Power Consumption (Average / Maximum)	38 W / 40 W	43 W / 47 W
Heat Dissipation	138 BTU/hr	159 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	20% to 90% non-condensing	10% to 90% non-condensing
Noise Level	49 dBA	
Air Flow	Front to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certifications	USGv6/IPv6	

\* FortiOS 7.6.1+ is required for supporting up to 48 FSW. All prior releases support up to 32.

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

<sup>1</sup> IPsec VPN performance test uses AES256-SHA256.

<sup>2</sup> IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

<sup>3</sup> SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

<sup>4</sup> NGFW performance is measured with Firewall, IPS and Application Control enabled.

<sup>5</sup> Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.



# Subscriptions

Service Category	Service Offering	A-la-carte	Bundles				
			Enterprise Protection	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 <sup>1</sup> , AI-based Heuristic AV, FortiGate Cloud Sandbox	•	•	•	•		
	URL, DNS and Video Filtering — URL, DNS and Video <sup>1</sup> Filtering, Malicious Certificate	•	•	•			
	Anti-Spam		•	•			
	AI-based Inline Malware Prevention	•	•				
	Data Loss Prevention (DLP) <sup>2</sup>	•	•				
	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 <sup>2</sup>	•					
	Application Control			-----included with FortiCare Subscription-----			
Inline CASB <sup>1</sup>			-----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 <sup>3</sup>					•	
	FortiGate Cloud One Year Cloud-based Log Retention					•	
	FortiTelemetry Cloud					•	
NOC and SOC Services	FortiConverter Service for One Time Configuration Conversion	•	•				
	Managed FortiGate Service—Available 24x7, 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—24x7 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, GeolPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing			-----included with FortiCare Subscription-----			

1. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.

2. Full features available when running FortiOS 7.4.1.

3. Only supported on FortiGate models from the 100F onwards (F-series and all later series). See the [FortiSASE Ordering Guide](#) for supported models and corresponding user license allocations.

## FortiGuard AI-Powered Security Bundles for FortiGate



FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24x7x365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.



## Ordering Information

Product	SKU	Description
FortiGate 120G	FG-120G	18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, 4x 10GE SFP+ slots, SP5 hardware accelerated, dual AC power supplies.
FortiGate 121G	FG-121G	18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, 4x 10GE SFP+ slots, SP5 hardware accelerated, 480GB onboard SSD storage, dual AC power supplies.
<b>Transceivers</b>		
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.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 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, 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.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 30km Long Range	FN-TRAN-SFP+BD27	10GE 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	10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
<b>Cables</b>		
10 GE SFP+ Passive Direct Attach Cable 1m	FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 3m	FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 5m	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots.

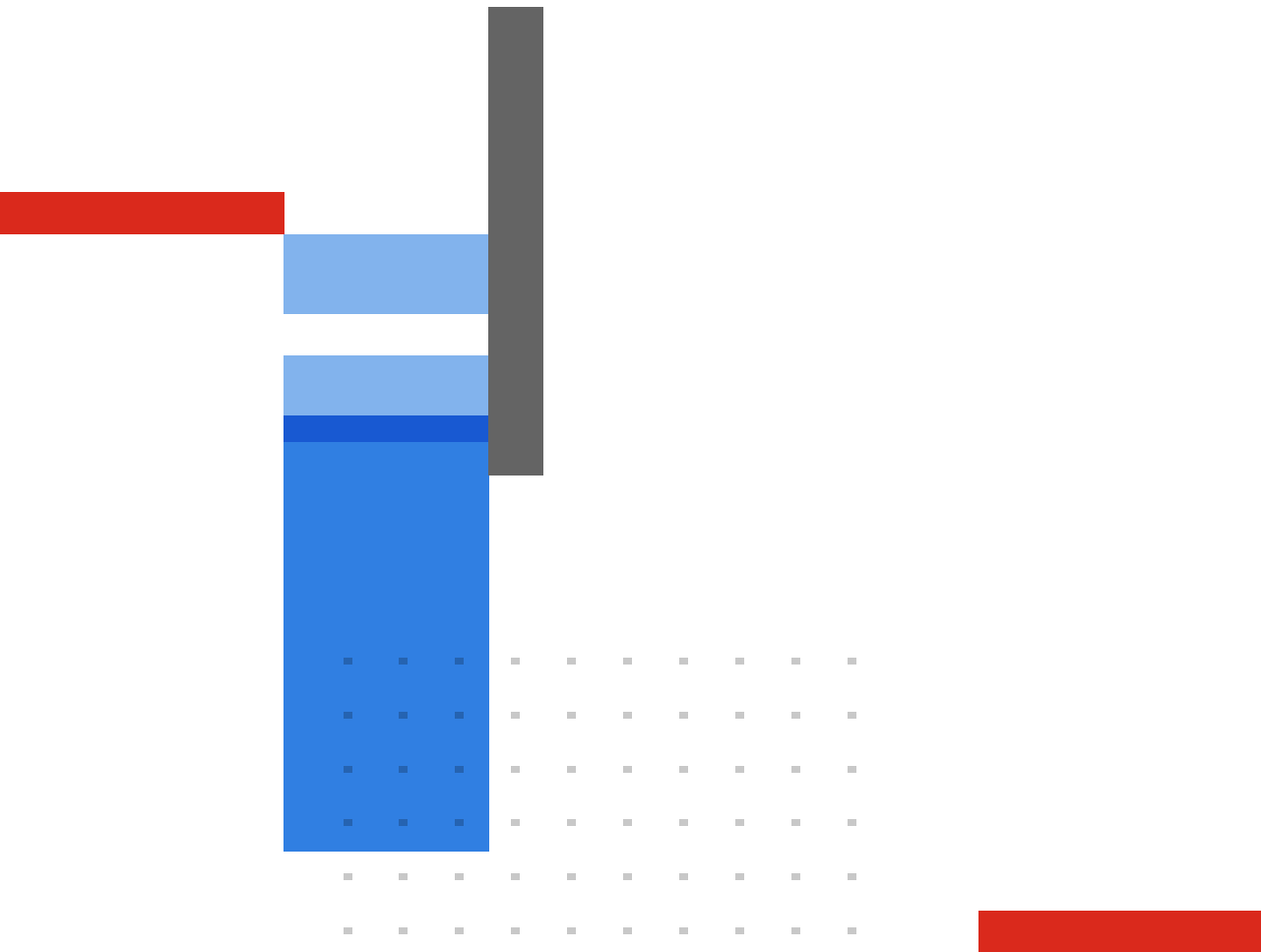
Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.



---

## Fortinet Corporate Social Responsibility Policy

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



[www.fortinet.com](http://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.