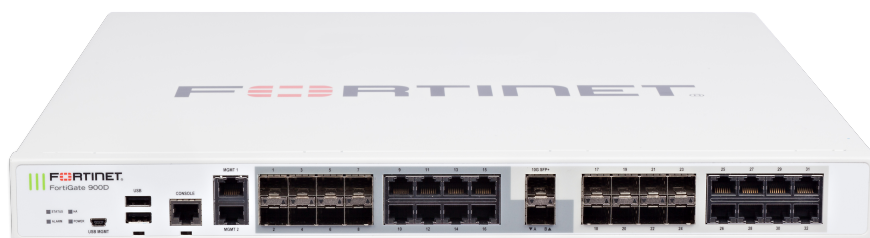


DATA SHEET

# FortiGate® 900D

FG-900D

Next Generation Firewall  
Secure SD-WAN  
Secure Web Gateway  
IPS



The FortiGate 900D series provides an application-centric, scalable and secure SD-WAN solution with next generation firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or enterprise branch level. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

## Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

## Performance

- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

## Certification

- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

## Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

## Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

## Security Fabric

- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

Firewall	IPS	NGFW	Threat Protection	Interfaces
52 Gbps	4.2 Gbps	4 Gbps	3 Gbps	Multiple GE RJ45, GE SFP, and 10 GE SFP+ slots

## DEPLOYMENT



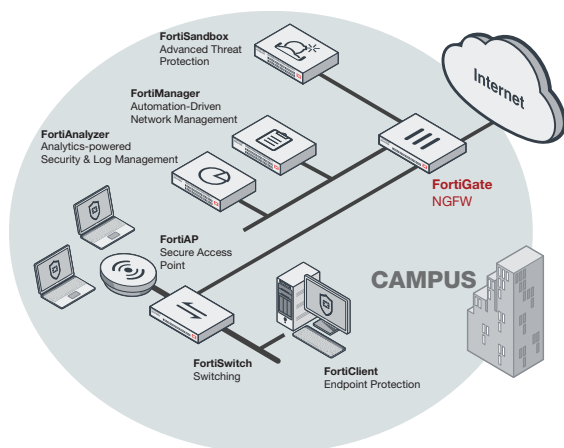
### Next Generation Firewall (NGFW)

- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the Industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric



### Secure Web Gateway (SWG)

- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL's and domains
- Prevent data loss and discover user activity to known and unknown cloud applications
- Block DNS requests against malicious domains
- Multi-layered advanced protection against zero-day malware threats delivered over the web



Next Generation Firewall Campus Deployment



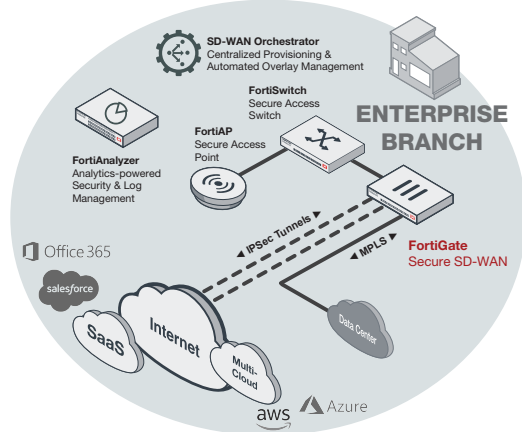
### Secure SD-WAN

- Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport
- Accelerated Multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based and real-time bandwidth compute-based traffic steering
- Automated Overlay tunnels provides encryption and abstracts physical hybrid WAN making it simple to manage.
- Simplified and intuitive workflow with SD-WAN Orchestrator for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identify anomalies
- Strong security posture with next generation firewall and real-time threat protection



### IPS

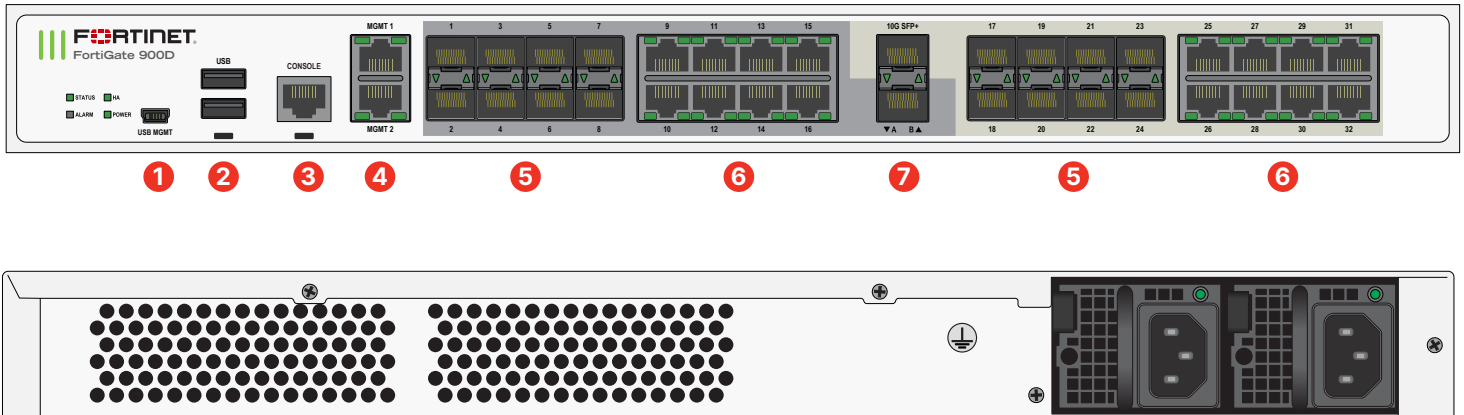
- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric



Secure SD-WAN Enterprise Branch Deployment

# HARDWARE

## FortiGate 900D



## Interfaces

1. USB Management Port
2. USB Ports
3. Console Port
4. 2x GE RJ45 Management Ports
5. 16x GE SFP Slots
6. 16x GE RJ45 Ports
7. 2x 10 GE SFP+ Slots

## NP Direct

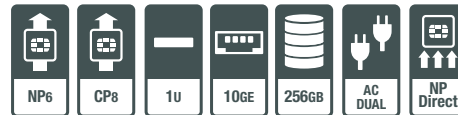
By removing the Internal Switch Fabric, the NP Direct architecture provides direct access to the SPU-NP for the lowest latency forwarding. NGFW deployments require some attention to network design to ensure optimal use of this technology.

### Powered by SPU

- Fortinet's custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck



## Hardware Features



## Network Processor

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

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

## Content Processor

Fortinet's ninth generation custom SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection.

## High-Speed Connectivity

High-speed connectivity is essential for network security segmentation. The FortiGate 900D provides 10 GE slots that simplify network designs without relying on additional devices to bridge desired connectivity.



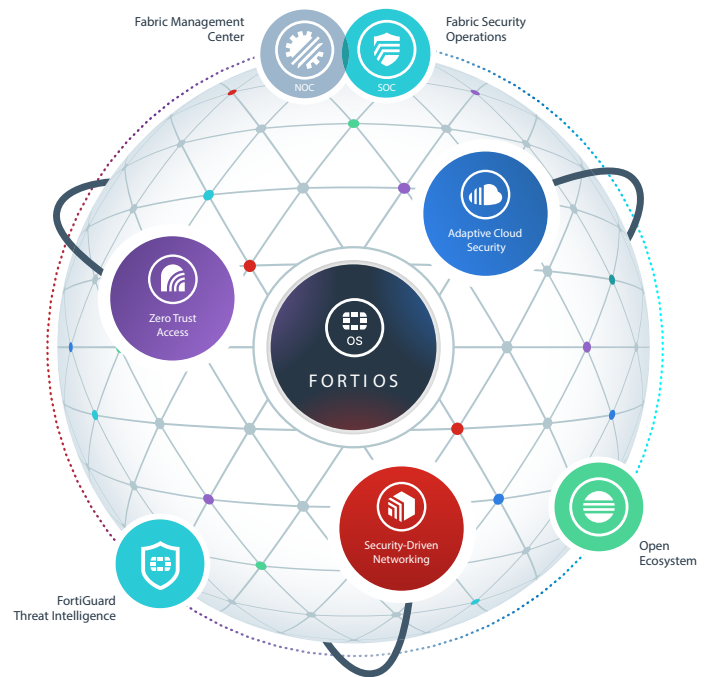
## FORTINET SECURITY FABRIC

### Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad:** Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated:** Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated:** Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



### FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models consisting on appliances, software and As-a-Service with SASE, ZTNA and other emerging cybersecurity solutions.

## SERVICES

### FortiGuard™ Security Services

FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.

### FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1,000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.

# SPECIFICATIONS

FORTIGATE 900D	
<b>Interfaces and Modules</b>	
Hardware Accelerated 10 GE SFP+ Slots	2
Hardware Accelerated GE SFP Slots	16
Hardware Accelerated GE RJ45 Ports	16
GE RJ45 Management / HA Ports	2
USB Ports (Client / Server)	1 / 2
Console Port	1
Onboard Storage	1x 256 GB SSD
Included Transceivers	0
<b>System Performance — Enterprise Traffic Mix</b>	
IPS Throughput <sup>2</sup>	4.2 Gbps
NGFW Throughput <sup>2,4</sup>	4 Gbps
Threat Protection Throughput <sup>2,5</sup>	3 Gbps
<b>System Performance and Capacity</b>	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	52 / 52 / 33 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	52 / 52 / 33 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	49.5 Mpps
Concurrent Sessions (TCP)	11 Million
New Sessions/Second (TCP)	280,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte) <sup>1</sup>	25 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	50,000
SSL-VPN Throughput	3.6 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	3.9 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	2,400
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	800,000
Application Control Throughput (HTTP 64K) <sup>2</sup>	10 Gbps
CAPWAP Throughput (1444 byte, UDP)	11 Gbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of FortiSwitches Supported	64
Maximum Number of FortiAPs (Total / Tunnel)	1024 / 512
Maximum Number of FortiTokens	5,000
High Availability Configurations	Active-Active, Active-Passive, Clustering

FORTIGATE 900D	
<b>Dimensions and Power</b>	
Height x Width x Length (inches)	1.75 × 17.22 × 18.24
Height x Width x Length (mm)	44.45 × 437.5 × 463.2
Weight	20.24 lbs (9.18 kg)
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 1 RU
Power Input	100–240V AC, 50/60 Hz, 300 W Redundant
Power Consumption (Average / Maximum)	135 W / 187.2 W
Current (Maximum)	100V/5A, 240V/3A
Heat Dissipation	638.75 BTU/h
Redundant Power Supplies	Yes (Hot Swappable)
<b>Operating Environment and Certifications</b>	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Humidity	10–90% non-condensing
Noise Level	49.9 dBA
Forced Airflow	Side to Back
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6

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

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

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



ORDERING INFORMATION

Product	SKU	Description
FortiGate 900D	FG-900D	2× 10 GE SFP+ slots, 16x GE SFP slots, 16x GE RJ45 ports, 2x GE RJ45 Management ports, SPU NP6 and CP8 hardware accelerated, 1× 256 GB SSD onboard storage, dual AC power supplies.
Optional Accessories/Spares	SKU	Description
1 GE SFP LX Transceiver Module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FG-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	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.
AC Power Supply	SP-FXX1000D	AC power supply for FG-900D, FG-1000D and FXX-1000D.

BUNDLES



FortiGuard Bundle

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.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	ASE <sup>1</sup>	24×7	24×7	24×7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video <sup>2</sup> Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard IoT Detection Service	•	•		
FortiGuard Industrial Service	•	•		
FortiConverter Service	•	•		
SD-WAN Orchestrator Entitlement	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
Fortinet SOCaaS	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

1. 24×7 plus Advanced Services Ticket Handling    2. Available when running FortiOS 7.0



www.fortinet.com

Copyright © 2021 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 General Counsel, 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.