

DATA SHEET

FortiGate® 100F Series

FortiGate 100F and 101F

 Next Generation Firewall
 Secure SD-WAN
 Secure Web Gateway


The FortiGate 100F 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 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
- Prevents and detects against known attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services
- Proactively blocks unknown sophisticated attacks in real-time with the Fortinet Security Fabric integrated AI-powered FortiSandbox

Performance

- Engineered for innovation using Fortinet's purpose-built security processors (SPU) to deliver the industry's best threat protection performance and ultra-low latency
- Provides industry-leading performance and protection for SSL encrypted traffic including the first firewall vendor to provide TLS 1.3 deep inspection

Certification

- Independently tested and validated best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs, ICASA, Virus Bulletin, and AV Comparatives

Networking

- Dynamic Path Selection over any WAN transport to provide better application experience based on self-healing SD-WAN capabilities
- Advanced routing, scalable VPN, multi-cast, and IPV4/IPV6 forwarding powered by purpose-built network processors

Management

- SD-WAN orchestration provides intuitive and simplified workflow for centralized management and provisioning of business policies in a few easy clicks
- Expedited deployment with zero touch provisioning well-suited for large and distributed infrastructure
- Automated VPN tunnels for flexible hub-to-spoke and full-mesh deployment at scale to provide bandwidth aggregation and encrypted WAN paths
- Predefined compliance checklists analyze the deployment and highlight best practices to improve the 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
- Automatically builds Network Topology visualizations which discover IoT devices and provide complete visibility into Fortinet and Fabric-ready partner products

Firewall	IPS	NGFW	Threat Protection	Interfaces
20 Gbps	2.6 Gbps	1.6 Gbps	1 Gbps	Multiple GE RJ45, GE SFP and 10 GE SFP+ slots

Refer to the specifications table for details

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, and 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



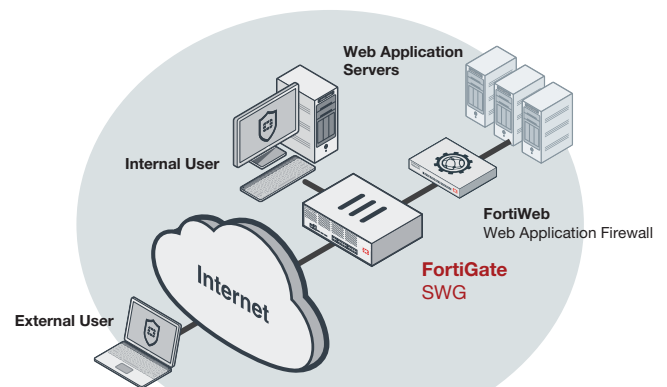
Secure Web Gateway (SWG)

- 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 URLs 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

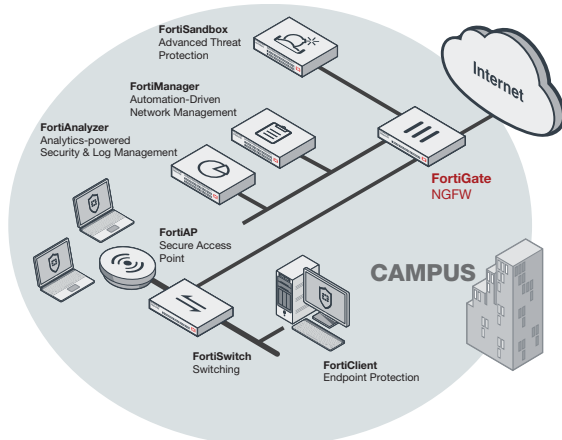


Secure SD-WAN

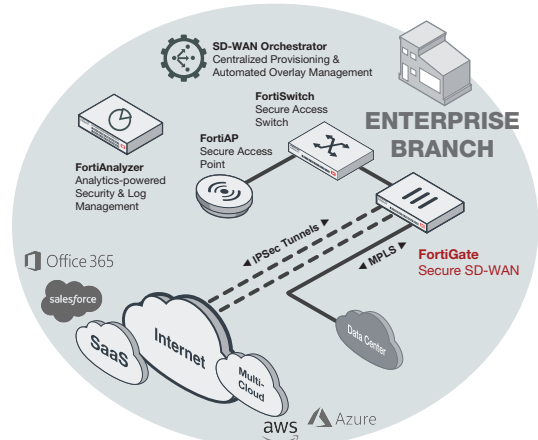
- Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport
- Accelerated multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based 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 identifies anomalies
- Strong security posture with next generation firewall and real-time threat protection



FortiGate 100F SWG deployment



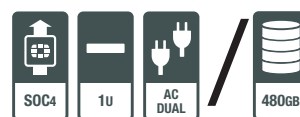
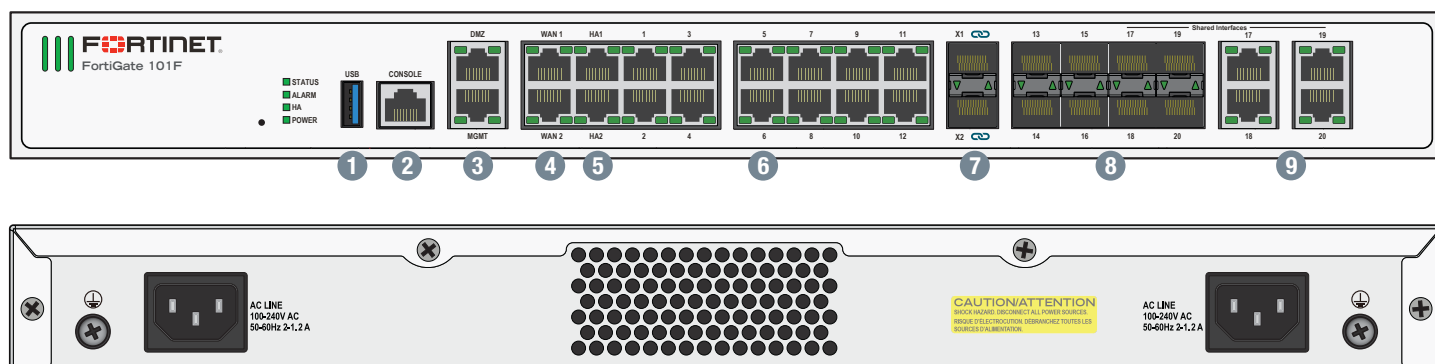
FortiGate 100F deployment in Campus (NGFW)



FortiGate 100F deployment in Enterprise Branch (Secure SD-WAN)

Hardware

FortiGate 100F/101F



Interfaces

- | | |
|-------------------------------|---------------------------------------|
| (1) 1x USB Port | (6) 12x GE RJ45 Ports |
| (2) 1x Console Port | (7) 2x 10 GE SFP+ FortiLink Slots |
| (3) 2x GE RJ45 MGMT/DMZ Ports | (8) 4x GE SFP Slots |
| (4) 2x GE RJ45 WAN Ports | (9) 4x GE RJ45/SFP Shared Media Pairs |
| (5) 2x GE RJ45 HA Ports | |

Powered by Purpose-built Secure SD-WAN ASIC SOC4



- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for 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

Dual Power Supplies

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 100F Series offers dual built-in non-hot swappable power supplies.

Extends Security to Access Layer with FortiLink Ports

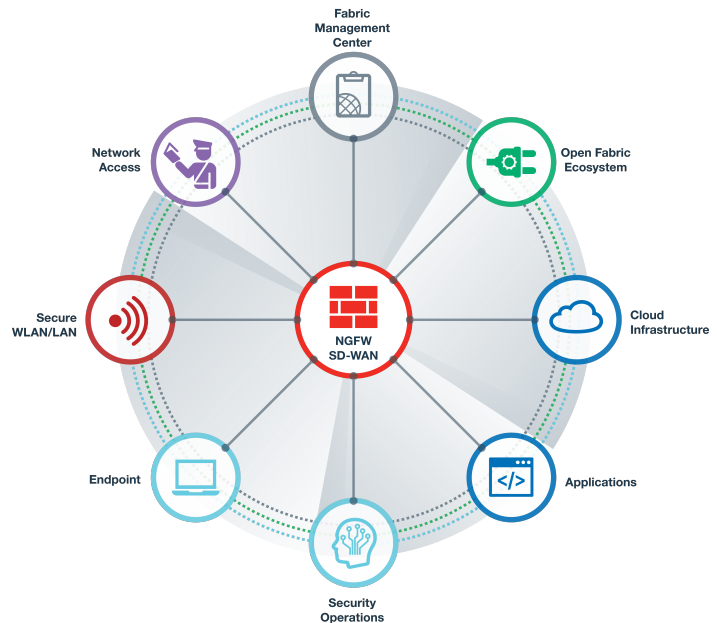
FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

Fortinet Security Fabric

Security Fabric

The Security Fabric is the cybersecurity platform that enables digital innovations. It delivers broad visibility of the entire attack surface to better manage risk. Its unified and integrated solution reduces the complexity of supporting multiple-point products, while automated workflows increase operational speeds and reduce response times across the Fortinet deployment ecosystem. The Fortinet Security Fabric covers the following key areas under a single management center:

- **Security-Driven Networking** that secures, accelerates, and unifies the network and user experience
- **Zero Trust Network Access** that identifies and secures users and devices in real-time, on and off of the network
- **Dynamic Cloud Security** that protects and controls cloud infrastructures and applications
- **AI-Driven Security Operations** that automatically prevents, detects, isolates, and responds to cyber threats



FortiOS

FortiGate is the foundation of the Fortinet Security Fabric—the core is FortiOS. All security and networking capabilities across the entire FortiGate platform are controlled with one intuitive operating system. FortiOS reduces complexity, costs, and response times by truly consolidating next-generation security products and services into one platform.

- A truly consolidated platform with a single OS and pane-of-glass across the entire digital attack surface
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSCA validated security and performance
- Leverage the latest technologies such as deception-based security

- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings in addition to true TLS 1.3 support
- Automatically prevent, detect, and mitigate advanced attacks within minutes with an integrated AI-driven security and advanced threat protection
- Improve and unify the user experience with innovative SD-WAN capabilities with the ability to detect, contain, and isolate threats with automated segmentation
- Utilize SPU hardware acceleration to boost network security performance

Services



FortiGuard™ Security Services

FortiGuard Labs offer 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™ Support Services

Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East, and Asia, FortiCare offers services to meet the needs of enterprises of all sizes.



For more information, please refer to forti.net/fortiguard and forti.net/forticare

Specifications

	FORTIGATE 100F	FORTIGATE 101F
Hardware Specifications		
GE RJ45 Ports	12	
GE RJ45 Management/HA/DMZ Ports	1 / 2 / 1	
GE SFP Slots	4	
10GE SFP+ FortiLink Slots (default)	2	
GE RJ45 WAN Ports	2	
GE RJ45 or SFP Shared Ports *	4	
USB Port	1	
Console Port	1	
Internal Storage	—	1x 480 GB SSD
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput ²	2.6 Gbps	
NGFW Throughput ^{2,4}	1.6 Gbps	
Threat Protection Throughput ^{2,5}	1 Gbps	
System Performance		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	20 / 18 / 10 Gbps	
Firewall Latency (64 byte UDP packets)	4.97 µs	
Firewall Throughput (Packets Per Second)	15 Mpps	
Concurrent Sessions (TCP)	1.5 Million	
New Sessions/Second (TCP)	56,000	
Firewall Policies	10,000	
IPsec VPN Throughput (512 byte) ¹	11.5 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2,500	
Client-to-Gateway IPsec VPN Tunnels	16,000	
SSL-VPN Throughput	1 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
SSL Inspection Throughput (IPS, avg. HTTPS) ³	1 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) ³	1,800	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	135,000	
Application Control Throughput (HTTP 64K) ²	2.2 Gbps	
CAPWAP Throughput (HTTP 64K)	15 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	24	
Maximum Number of FortiAPs (Total / Tunnel Mode)	128 / 64	
Maximum Number of FortiTokens	5,000	
High Availability Configurations	Active / Active, Active / Passive, Clustering	

	FORTIGATE 100F	FORTIGATE 101F
Dimensions		
Height x Width x Length (inches)	1.73 x 17 x 10	
Height x Width x Length (mm)	44 x 432 x 254	
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 1 RU	
Weight	7.25 lbs (3.29 kg)	7.56 lbs (3.43 kg)
Environment		
Power Required	100–240V AC, 50-60	
Maximum Current	100V / 1A, 240V / 0.5A	
Power Consumption (Average / Maximum)	35.1 W / 38.7 W	35.3 W / 39.1 W
Heat Dissipation	119.77 BTU/h	121.13 BTU/h
Redundant Power Supplies	Yes	
Environment		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Humidity	10–90% non-condensing	
Noise Level	40.4 dBA	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; IPv6	

* Copper SFP module is not supported.

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.

Order Information

Product	SKU	Description
FortiGate 100F	FG-100F	22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10 GE SFP+ FortiLinks, dual power supplies redundancy
FortiGate 101F	FG-101F	22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10 GE SFP+ FortiLinks, 480GB onboard storage, dual power supplies redundancy
Optional Accessories		
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

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	Threat Protection
FortiCare	ASE ¹	24x7	24x7	24x7
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 Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard Industrial Service	•	•		
FortiGuard IoT Detection Service ²	•	•		
FortiConverter Service	•	•		
IPAM Cloud ²	•			
SD-WAN Orchestrator Entitlement ²	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

(1) 24x7 plus Advanced Services Ticket Handling (2) Available when running FortiOS 6.4

FORTINET



Corporate Armor

sales@corporatearmor.com

877.449.0458

Copyright © 2020 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. 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.