

FortiGate 70F Series

FG-70F and FG-71F



Highlights

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

Security-Driven Networking with FortiOS delivers converged networking and security.

Unparalleled Performance with Fortinet's patented SoC processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Simplified Operations with centralized management for networking and security, automation, deep analytics, and self-healing.

Converged Next-Generation Firewall (NGFW) and SD-WAN

The FortiGate Next-Generation Firewall 70F series is ideal for building security-driven networks at distributed enterprise sites and transforming WAN architecture at any scale.

With a rich set of AI/ML-based FortiGuard security services and our integrated Security Fabric platform, the FortiGate 70F series delivers coordinated, automated, end-to-end threat protection across all use cases.

FortiGate has the industry's first integrated SD-WAN and zero-trust network access (ZTNA) enforcement within an NGFW solution and is powered by one OS. FortiGate 70F automatically controls, verifies, and facilitates user access to applications, delivering consistency with a seamless and optimized user experience.

IPS	NGFW	Threat Protection	Interfaces
1.4 Gbps	1 Gbps	800 Mbps	Multiple GE RJ45 Variants with internal storage



Available in



Appliance



Virtual



Hosted



Cloud



Container

FortiOS Everywhere

FortiOS, Fortinet's advanced operating system

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

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

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

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of a simplified, single policy and management framework. Its security policies enable centralized management across large-scale networks with the following key attributes:

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



Intuitive easy to use view into the network and endpoint vulnerabilities

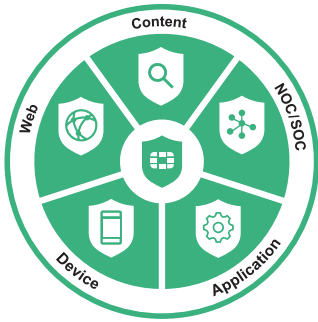


Visibility with FOS Application Signatures

FortiConverter Service

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





FortiGuard Services

FortiGuard AI-Powered Security

FortiGuard's rich suite of security services counter threats in real time using AI-powered, coordinated protection designed by FortiGuard Labs security threat researchers, engineers, and forensic specialists.

Web Security

Advanced cloud-delivered URL, DNS (Domain Name System), and Video Filtering providing complete protection for phishing and other web born attacks while meeting compliance.

Additionally, its dynamic inline CASB (Cloud Access Security Broker) service is focused on securing business SaaS data, while inline ZTNA traffic inspection and ZTNA posture check provide per-sessions access control to applications. It also integrates with the FortiClient Fabric Agent to extend protection to remote and mobile users.

Content Security

Advanced content security technologies enable the detection and prevention of known and unknown threats and file-based attack tactics in real-time. With capabilities like CPRL (Compact Pattern Recognition Language), AV, inline Sandbox, and lateral movement protection make it a complete solution to address ransomware, malware, and credential-based attacks.

Device Security

Advanced security technologies are optimized to monitor and protect IT, IIoT, and OT (Operational Technology) devices against vulnerability and device-based attack tactics. Its validated near-real-time IPS intelligence detects, and blocks known and zero-day threats, provides deep visibility and control into ICS/OT/SCADA protocols, and provides automated discovery, segmentation, and pattern identification-based policies.

Advanced Tools for SOC/NOC

Advanced NOC and SOC management tools attached to your NGFW provide simplified and faster time-to-activation.

SOC-as-a-Service

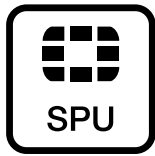
Includes tier-one hunting and automation, log location, 24x7 SOC analyst experts, managed firewall and endpoint functions, and alert triage.

Fabric Rating Security Best Practices

Includes supply chain virtual patching, up-to-date risk and vulnerability data to deliver quicker business decisions, and remediation for data breach situations.



Secure Any Edge at Any Scale



Powered by Security Processing Unit (SPU)

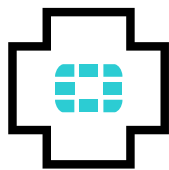
Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and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

ASIC Advantage



Secure SD-WAN ASIC SOC4

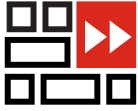
- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience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



FortiCare Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.

Use Cases



Next Generation Firewall (NGFW)

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



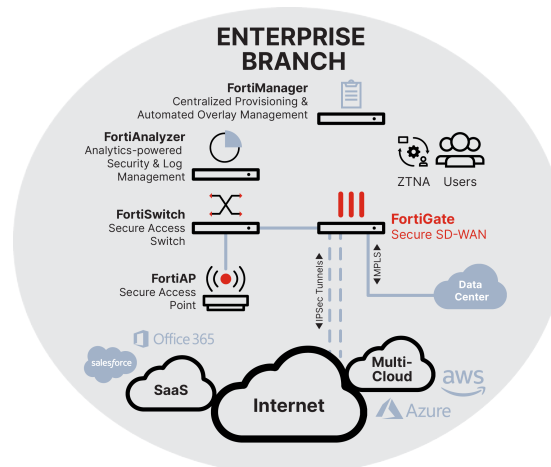
Secure SD-WAN

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



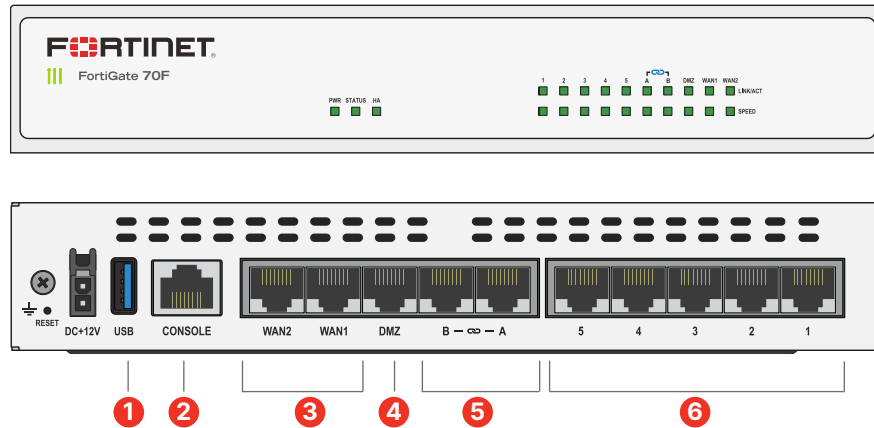
Universal ZTNA

- 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



Hardware

FortiGate 70F/71F



Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 WAN Ports
4. 1 x GE RJ45 DMZ Port
5. 2 x GE RJ45 FortiLink Ports
6. 5 x GE RJ45 Internal Ports

Hardware Features



Specifications

	FORTIGATE 70F	FORTIGATE 71F
Hardware Specifications		
GE RJ45 WAN / DMZ Ports	2 / 1	2 / 1
GE RJ45 Internal Ports	5	5
GE RJ45 FortiLink Ports (Default)	2	2
Wireless Interface	–	–
USB Ports	1	1
Console (RJ45)	1	1
Internal Storage	–	1 × 128 GB SSD
Trusted Platform Module (TPM)	No	No
Bluetooth Low Energy (BLE)	No	No
System Performance* — Enterprise Traffic Mix		
IPS Throughput ²		1.4 Gbps
NGFW Throughput ^{2,4}		1 Gbps
Threat Protection Throughput ^{2,5}		800 Mbps
System Performance and Capacity		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)		10/10/6 Gbps
Firewall Latency (64 byte UDP packets)		2.54 μs
Firewall Throughput (Packets Per Second)		9 Mpps
Concurrent Sessions (TCP)		1.5 M
New Sessions/Second (TCP)		35 000
Firewall Policies		5000
IPsec VPN Throughput (512 byte) ¹		6.1 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		200
Client-to-Gateway IPsec VPN Tunnels		500
SSL-VPN Throughput ⁶		405 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		200
SSL Inspection Throughput (IPS, avg. HTTPS) ³		700 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) ³		500
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³		100 000
Application Control Throughput (HTTP 64K) ²		1.8 Gbps
CAPWAP Throughput (HTTP 64K)		8.5 Gbps
Virtual Domains (Default / Maximum)		10 / 10
Maximum Number of FortiSwitches Supported		16
Maximum Number of FortiAPs (Total / Tunnel Mode)		64 / 32
Maximum Number of FortiTokens		500
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 70F	FORTIGATE 71F
Dimensions		
Height x Width x Length (inches)	1.5 × 8.5 × 6.3	
Height x Width x Length (mm)	38.5 × 216 × 160 mm	
Weight	2.23 lbs (1.01 kg)	
Form Factor	Desktop	
Operating Environment and Certifications		
Power Rating	12VDC, 3A	
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz	
Maximum Current	100VAC/1.0A, 240VAC/0.6A	
Power Consumption (Average / Maximum)	10.17 W / 12.43 W	17.2 W / 18.7 W
Heat Dissipation	63.1 BTU/hr	63.8 BTU/hr
Operating Temperature	32°–104°F (0°–40°C)	
Storage Temperature	–31°–158°F (–35°–70°C)	
Humidity	Humidity 10%–90% non-condensing	
Noise Level	Fanless 0 dBA	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN	

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.

⁶ Uses RSA-2048 certificate.



SUBSCRIPTIONS

Service Category	Service Offering	A-la-carte	Bundles			
			Enterprise Protection	SMB Protection	Unified Threat Protection	Advanced Threat Protection
Security Services	FortiGuard IPS Service	•	•	•	•	•
	FortiGuard Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•	•
	FortiGuard Web Security — URL and web content, Video and Secure DNS Filtering	•	•	•	•	•
	FortiGuard Anti-Spam	•	•	•	•	•
	FortiGuard IoT Detection Service	•	•	•	•	•
	FortiGuard Industrial Security Service	•	•	•	•	•
	FortiCloud AI-based Inline Sandbox Service ¹	•	•	•	•	•
NOC Services	FortiGate Cloud (SMB Logging + Cloud Management)	•	•	•	•	•
	FortiGuard Security Fabric Rating and Compliance Monitoring Service	•	•	•	•	•
	FortiConverter Service	•	•	•	•	•
	FortiGuard SD-WAN Underlay Bandwidth and Quality Monitoring Service	•	•	•	•	•
SOC Services	FortiAnalyzer Cloud	•	•	•	•	•
	FortiAnalyzer Cloud with SOCaas	•	•	•	•	•
Hardware and Software Support	FortiCare Essentials	•	•	•	•	•
	FortiCare Premium	•	•	•	•	•
	FortiCare Elite	•	•	•	•	•
Base Services	FortiGuard Application Control	•	•	•	•	•
	FortiCloud ZTNA Inline CASB Service ¹	•	•	•	•	•
	Internet Service (SaaS) DB Updates	•	•	•	•	•
	GeoIP DB Updates	•	•	•	•	•
	Device/OS Detection Signatures	•	•	•	•	•
	Trusted Certificate DB Updates	•	•	•	•	•
	DDNS (v4/v6) Service	•	•	•	•	•

¹ Available when running FortiOS 7.2



FortiGuard Bundles

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

FortiCare Elite

FortiCare Elite services offers enhanced service-level agreements (SLAs) and accelerated issue resolution. This advanced support offering provides access to a dedicated support team. Single-touch ticket handling by the expert technical team streamlines resolution. This option also provides Extended End-of-Engineering-Support (EoE's) of 18 months for added flexibility and access to the new FortiCare Elite Portal. This intuitive portal provides a single unified view of device and security health.

Fortinet CSR Policy

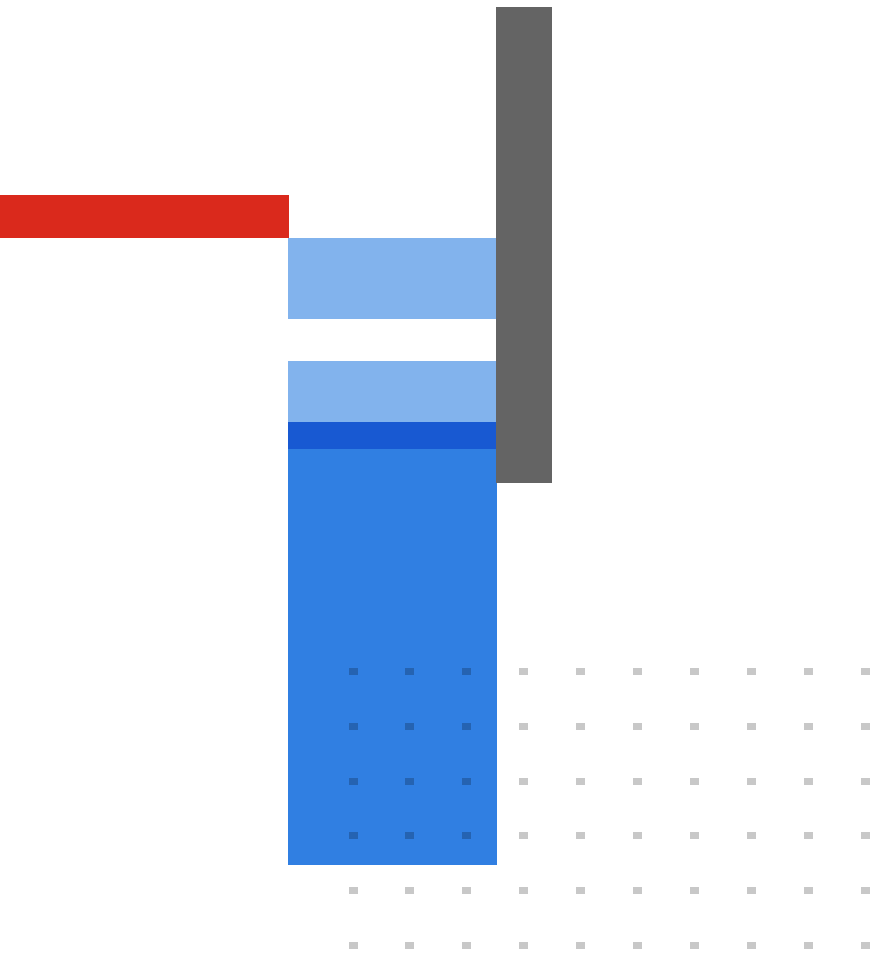
Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services 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](#).



Ordering Information

Product	SKU	Description
FortiGate 70F	FG-70F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port).
FortiGate 71F	FG-71F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage.
Optional Accessories		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01.
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, FG/FWF 60F/61F, FG-70F/71F, and FG-80E/81E.
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-60F, FG-70F/71F and FG/FWF-80F series.





FORTINET

www.fortinet.com

Copyright © 2022 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.

December 7, 2022

FG-70F-DAT-R03-20221207