Saved from manuals.plus.
Open the live page for links to other documents and user manuals.

FORTINET FG-60F

FortiGate-60F Firewall Appliance User Manual

Model: FG-60F

1. Product Overview

The FortiGate-60F is a high-performance firewall appliance designed to provide robust network security for various enterprise networking needs. It integrates advanced security features with extensive connectivity options to ensure secure and efficient network operations.



Figure 1: Front view of the FortiGate-60F Firewall Appliance.

Key Features:

- **Extensive Connectivity Options:** Features 10 GE RJ45 ports, including 2 WAN ports, 1 DMZ port, and 7 internal ports for broad flexibility.
- **Superior Performance:** Delivers 1.4 Gbps IPS throughput and 700 Mbps threat protection throughput via system-on-a-chip acceleration.
- **Enhanced SSL Inspection and SD-WAN:** Utilizes purpose-built security processor technology for high SSL inspection performance and robust SD-WAN functionality.
- **Simple and Effective Management:** User-friendly management console with comprehensive network automation and Zero Touch Integration with Fortinet's Security Fabric.
- **Advanced Security:** Leverages continuous threat intelligence from AI-powered FortiGuard Labs to mitigate known and unknown threats.

2. Setup Guide

This section provides instructions for the initial setup of your FortiGate-60F appliance.

2.1 Unpacking and Physical Placement

Carefully remove the FortiGate-60F appliance from its packaging. Ensure all components are present. Place the appliance on a stable, flat surface with adequate ventilation to prevent overheating. The compact design allows for flexible placement in various environments.



Figure 2: FortiGate-60F dimensions. The appliance measures approximately 11 x 5 x 8 inches and weighs 2 pounds.

2.2 Connecting the Appliance

Identify the various ports on the rear of the FortiGate-60F. These include USB, Console, WAN, DMZ, and internal RJ45 ports.

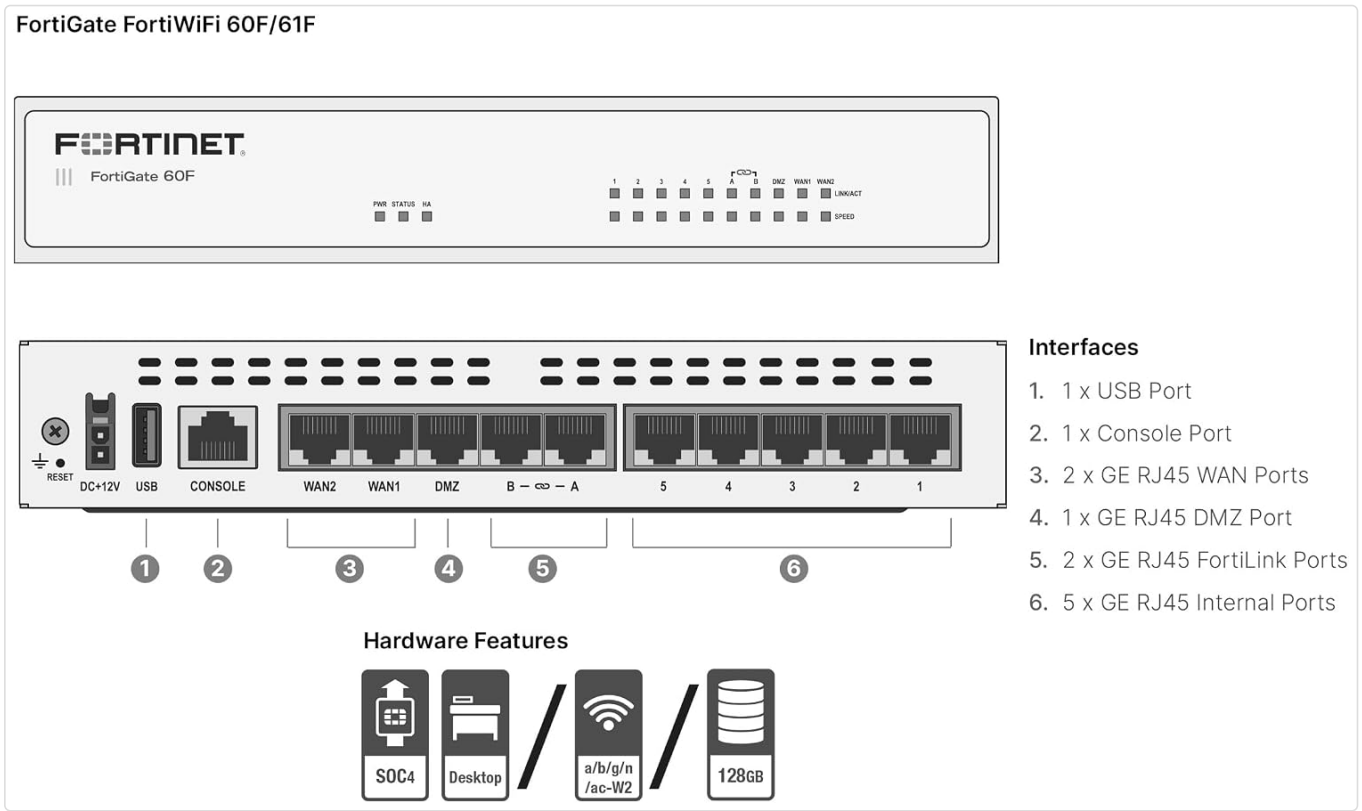

Figure 3: Rear view of the FortiGate-60F showing port layout. Ports include USB, Console, WAN1, WAN2, DMZ, and internal GE RJ45 ports (1-7).

1. **Power Connection:** Connect the provided power adapter to the DC 12V port on the appliance and then to a power outlet.
2. **WAN Connection:** Connect your internet service provider's modem or router to one of the WAN ports (WAN1 or WAN2) using an Ethernet cable.
3. **LAN Connection:** Connect your internal network devices (e.g., computers, switches) to the internal RJ45 ports (1-7).

4. **Console Connection (Optional):** For initial configuration or troubleshooting, connect a computer to the Console port using a console cable.
5. **USB Port (Optional):** The USB port can be used for external storage or other supported peripherals.

2.3 Initial Configuration

After connecting the hardware, you can proceed with the initial software configuration. This typically involves accessing the device's web-based management interface or using the command-line interface (CLI) via the console port.

- Refer to the Fortinet documentation for detailed steps on accessing the management interface and performing initial network settings, including IP address assignment, DHCP configuration, and basic firewall rules.
- The appliance supports Zero Touch Integration with Fortinet's Security Fabric for streamlined deployment in larger environments.

3. Operating Instructions

The FortiGate-60F operates as a central point for network security, inspecting and controlling traffic based on configured policies. Its powerful system-on-a-chip acceleration ensures high throughput for various security functions.

3.1 Security Fabric Integration

The FortiGate-60F is designed to integrate seamlessly into the Fortinet Security Fabric, providing broad visibility and protection across the entire digital attack surface. This integration allows for centralized management and shared threat intelligence, enhancing overall security posture.

3.2 Threat Protection and SD-WAN

The appliance provides robust threat protection, including Intrusion Prevention System (IPS), antivirus, and web filtering, powered by continuous threat intelligence from FortiGuard Labs. It also offers advanced SD-WAN capabilities for optimizing network performance and ensuring secure, high-speed connectivity for distributed environments.

3.3 SSL Inspection

With purpose-built security processor technology, the FortiGate-60F delivers high SSL inspection performance, allowing for the inspection of encrypted traffic to detect and mitigate hidden threats without compromising network speed.

4. Maintenance

Regular maintenance is crucial for ensuring the optimal performance and security of your FortiGate-60F appliance.

4.1 Firmware Updates

Fortinet regularly releases firmware updates that include new features, performance enhancements, and critical security patches. It is highly recommended to keep your appliance's firmware up to date. Firmware updates may require an active support contract.

4.2 Security Service Subscriptions

To maintain comprehensive threat protection, ensure your FortiGuard security service subscriptions are active. These subscriptions provide real-time threat intelligence, including updates for antivirus, IPS, web filtering, and other security features.

Subscriptions

			Bundles		
Service Category	Service Offering	A-la-carte	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service [1]	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) [1]	•			
	Application Control		included with FortiCare Subscription		
	CASB SaaS Control		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license [2]	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Internet Service (SaaS) DB Updates	included with FortiCare Subscription			
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Full features available when running FortiOS 7.4.1
2. Desktop Models only

Figure 4: Overview of FortiGuard and FortiCare service categories and offerings.

4.3 Backup Configuration

Regularly back up your appliance's configuration. This allows for quick restoration of settings in case of an unexpected issue or hardware replacement.

5. Troubleshooting

This section provides general guidance for common issues. For detailed troubleshooting, refer to the official Fortinet documentation or contact technical support.

5.1 Connectivity Issues

- **No Internet Access:** Verify WAN cable connection, check ISP modem status, and ensure correct WAN interface configuration on the FortiGate.
- **Local Network Access:** Confirm LAN cable connections, check IP address settings on connected devices, and

review internal port configurations.

5.2 Performance Degradation

- **Slow Throughput:** Check CPU and memory utilization via the management interface. Ensure security policies are optimized and not causing excessive resource consumption.
- **High Latency:** Investigate potential network bottlenecks or misconfigurations.

5.3 Accessing Management Interface

- **Cannot Log In:** Verify username and password. If forgotten, follow the password recovery procedure outlined in the official documentation.
- **Interface Unreachable:** Ensure your computer is on the correct network segment and that there are no IP address conflicts.

6. Specifications

The following table outlines the key technical specifications of the FortiGate-60F Firewall Appliance.

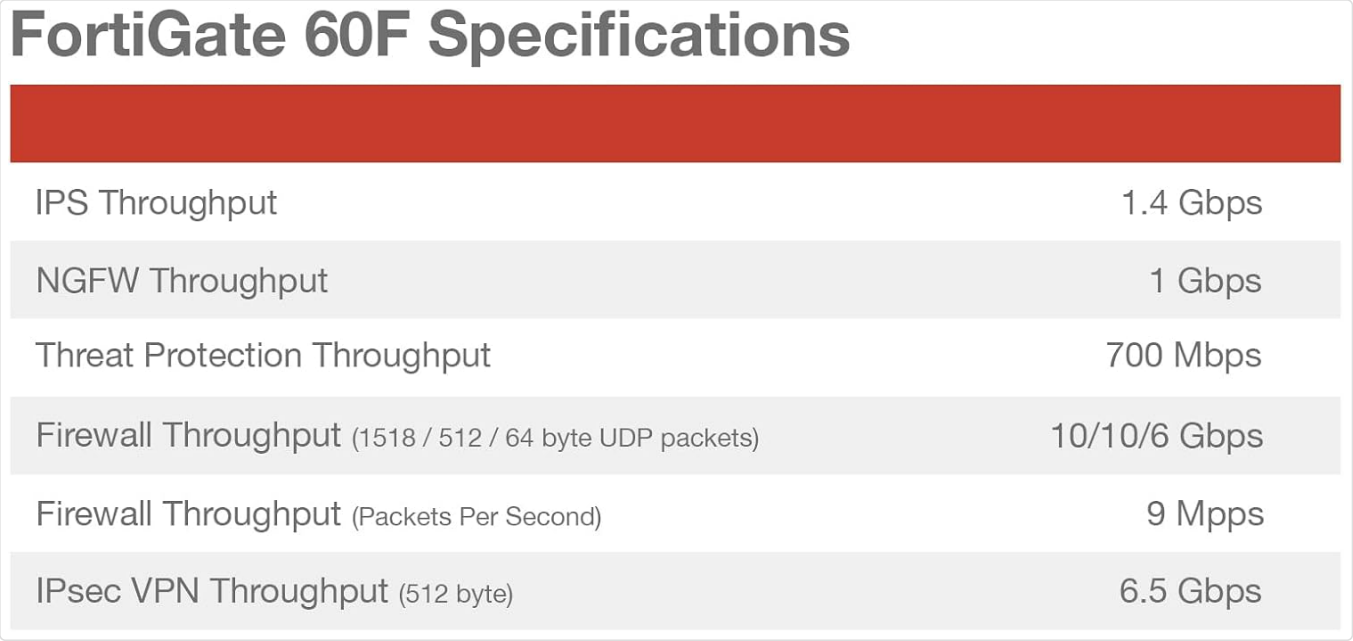

Figure 5: FortiGate-60F performance specifications.

Attribute	Value
Product Dimensions	11 x 5 x 8 inches
Item Weight	2 pounds
Model Number	FG-60F
Manufacturer	Fortinet
Connectivity Technology	RJ45
Ports	10 x GE RJ45 (2 WAN, 1 DMZ, 7 Internal)

Attribute	Value
IPS Throughput	1.4 Gbps
Threat Protection Throughput	700 Mbps
Firewall Throughput (1518/512/64 byte UDP packets)	10/10/6 Gbps
IPsec VPN Throughput (512 byte)	6.5 Gbps

7. Warranty and Support

Fortinet provides various support options and warranty coverage for its products.

7.1 Warranty Information

The FortiGate-60F appliance typically comes with a standard hardware warranty. For specific details regarding your product's warranty period and terms, please refer to the documentation included with your purchase or visit the official Fortinet website.

7.2 Technical Support and Services

Fortinet offers comprehensive technical support and various service bundles, including FortiCare Premium, to ensure optimal operation and protection. These services often include access to firmware updates, technical assistance, and advanced threat intelligence updates from FortiGuard Labs.

Note: Access to certain updates, patches, and technical support services may require an active paid subscription or support contract. Please review the terms of your FortiCare or FortiGuard subscription for full details.

For further assistance, visit the official Fortinet support portal:support.fortinet.com

© 2024 FORTINET. All rights reserved.

Ask a question about this manual

Ask about setup, troubleshooting, compatibility, parts, safety, or missing instructions. Manuals+ will review the question and use this page's manual context to help answer it.

Name

Anonymous

Email

you@example.com

After a successful submission, we securely hash the supplied account or form email before sending it to Microsoft Advertising for conversion attribution. Privacy details.

Question

Example: How do I reset this device or fix this error?

Details

Model number, symptoms, what you tried, or the section of the manual you are using.

Submit question

Open the live page

https://manuals.plus/asin/B07ZZMFWJ7

More documents and user manuals: **https://manuals.plus/**