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

FORTINET FG-60F-BDL-950-12

FortiGate-60F Network Security Appliance User Manual

Model: FG-60F-BDL-950-12

1. Introduction

The FortiGate-60F Network Security Appliance provides robust, comprehensive threat protection for medium-sized businesses. This manual outlines the setup, operation, maintenance, and troubleshooting of your FortiGate-60F device, ensuring optimal performance and security.

It integrates advanced security features such as Unified Threat Protection (UTP) and FortiCare Premium support, offering a complete security solution against evolving cyber threats.

2. Product Overview

2.1 Key Features

- **HARDWARE PLUS SECURITY SERVICES:** FortiGate-60F Firewall Appliance bundled with 1 year of FortiCare Premium and FortiGuard Unified Threat Protection.
- **UNIFIED THREAT PROTECTION (UTP):** Secures against advanced online threats with comprehensive web filtering and anti-botnet technologies.
- **OPTIMIZED FOR MEDIUM-SIZED BUSINESSES:** Tailored for businesses needing robust security without the infrastructure of larger enterprises.
- **RELIABLE CUSTOMER SUPPORT:** FortiCare Premium ensures high-quality support and service continuity.
- **EFFECTIVE PROTECTION:** Employs advanced filtering technologies to safeguard against sophisticated threats.

2.2 Package Contents

Verify that all items are present in your package:

- FortiGate-60F Firewall Appliance
- FortiGate 60F NGFW
- FortiCare support documentation
- FortiGuard services activation information

2.3 Physical Overview



Figure 2.3.1: Front view of the FortiGate-60F appliance, showing status indicators and port labels.



Figure 2.3.2: Rear view of the FortiGate-60F appliance, highlighting the various ports including USB, Console, WAN, DMZ, and internal ports.

The FortiGate-60F features a compact design with clearly labeled ports and indicators on the front and rear panels. The front panel includes power, status, and HA indicators, along with link/activity and speed indicators for each port. The rear panel provides connectivity for power, USB, console, and multiple Ethernet ports for WAN, DMZ, and internal network connections.

3. Setup and Installation

3.1 Initial Setup

Before powering on the device, ensure proper physical connections.

1. **Connect Power:** Connect the provided power adapter to the DC 12V port on the rear of the FortiGate-60F and plug it into a power outlet.
2. **Network Connections:**
    - Connect your internet service provider's modem/router to one of the WAN ports (WAN1 or WAN2).
    - Connect your internal network devices (switches, computers) to the internal GE RJ45 ports (1-5).
    - If applicable, connect devices requiring a demilitarized zone (DMZ) to the DMZ port.
3. **Console Connection (Optional):** For direct management, connect a console cable from your computer to the Console port.

3.2 First-Time Configuration

The FortiGate-60F can be configured via local setup, cloud setup, or iOS app.

- **Local Setup:**
    a. Connect port 1 to your computer.
    b. Enable DHCP on your computer or set your IP to 192.168.1.1, subnet mask 255.255.0.0.
    c. Visit 192.168.1.99 in a web browser.
- **Cloud Setup:**
    a. Visit forticloud.com in a web browser and log in using your FortiNetOne credentials.
    b. Click Add FortiGate and enter the Cloud Key below.
- **iOS Setup:**
    a. Download and launch the FortiExplorer iOS App.
    b. Connect the USB port to your iOS device with an Apple Lightning to USB cable.
    c. Tap the device when it appears in FortiExplorer.

For detailed setup instructions, refer to the official Fortinet documentation or the setup video linked on the device's packaging.

4. Operating the FortiGate-60F

4.1 Management Interface

The FortiGate-60F is primarily managed through its web-based graphical user interface (GUI) or command-line interface (CLI).

- **Web GUI:** Accessible via a web browser, the GUI provides a comprehensive dashboard for monitoring, configuring security policies, network settings, and system status.
- **CLI:** For advanced configurations and troubleshooting, the CLI can be accessed via SSH, Telnet, or the console port.

4.2 Security Features

Leverage the FortiGate-60F's advanced security capabilities:

- **Firewall Policies:** Configure rules to control traffic flow between network segments.
- **Unified Threat Protection (UTP):** Activate and manage services like IPS, antivirus, web filtering, and anti-botnet

to protect against various threats.

- **VPN:** Establish secure remote access or site-to-site connections using IPsec or SSL VPN.
- **Application Control:** Identify and control applications on your network.
- **Intrusion Prevention System (IPS):** Detect and block malicious network activity.

5. Maintenance

5.1 Firmware Updates

Regularly update the device firmware to ensure optimal performance, security, and access to new features. Firmware updates are typically available through the FortiCloud portal or the Fortinet support website.

5.2 Configuration Backup and Restore

Periodically back up your device configuration to prevent data loss. This can be done via the web GUI or CLI. In case of a system failure or misconfiguration, you can restore a previous working configuration.

5.3 Monitoring and Logging

Utilize the FortiGate's logging and monitoring features to track network activity, security events, and system health. This helps in identifying potential issues and ensuring compliance.

6. Troubleshooting

6.1 Common Issues and Solutions

Issue	Possible Cause	Solution
No Internet Connectivity	Incorrect WAN configuration, ISP issue, cable problem.	Verify WAN settings, check physical cable connections, contact ISP.
Cannot Access Web GUI	Incorrect IP address, network connectivity issue, browser cache.	Ensure correct IP (192.168.1.99 default), clear browser cache, try different browser.
Slow Network Performance	High traffic, misconfigured policies, hardware limitations.	Review traffic logs, optimize security policies, check hardware specifications.

6.2 Resetting to Factory Defaults

If severe issues persist, you may need to reset the device to factory defaults. This will erase all configurations. Refer to the official documentation for the specific reset procedure for your model.

7. Specifications

Attribute	Value
Model Name	FG-60F-BDL-950-12
Product Dimensions	6.3 x 8.5 x 1.5 inches
Item Weight	0.01 ounces
Manufacturer	Fortinet
IPS Throughput	1.4 Gbps
NGFW Throughput	1 Gbps
Threat Protection Throughput	700 Mbps
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10/10/6 Gbps
Firewall Throughput (Packets Per Second)	9 Mpps
IPsec VPN Throughput (512 byte)	6.5 Gbps
Connectivity Technology	802.11ac, Ethernet
Included Components	FortiGate-60F Firewall Appliance, FortiGate 60F NGFW, FortiCare support, FortiGuard services

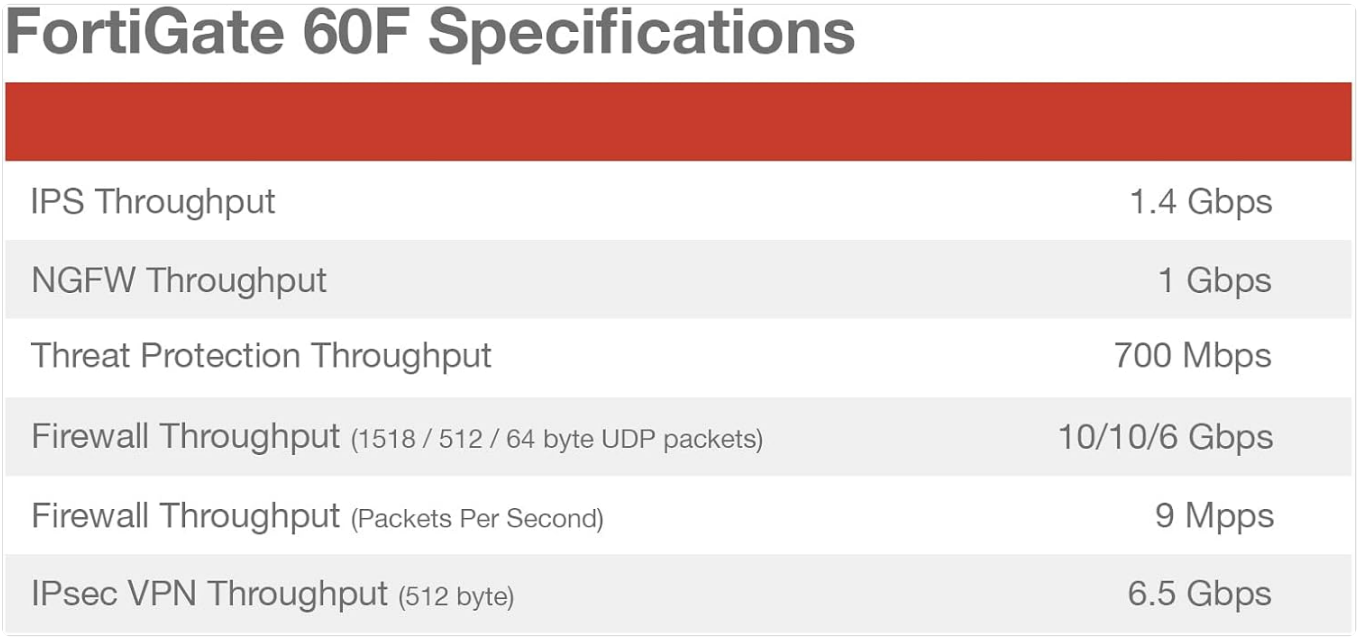

Figure 7.1: Detailed performance specifications for the FortiGate 60F, including IPS, NGFW, Threat Protection, Firewall, and IPsec VPN throughputs.

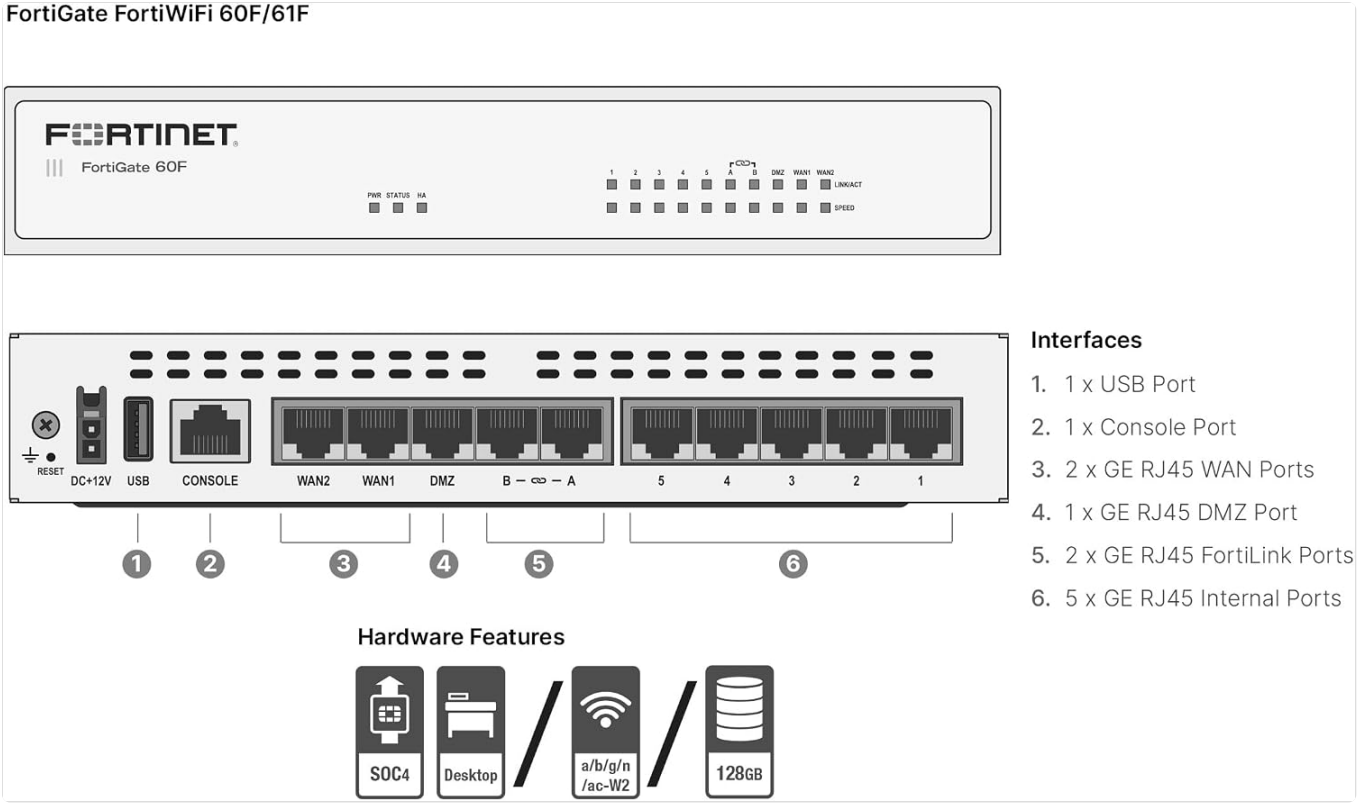

Figure 7.2: Hardware features and interface layout including USB, Console, WAN, DMZ, and internal ports.

8. Warranty and Support

8.1 FortiCare Premium Support

Your FortiGate-60F bundle includes 1 year of FortiCare Premium support. This service provides:

- 24x7 technical support
- Advanced hardware replacement
- Firmware and general upgrades
- Access to Fortinet support resources

For detailed information on your FortiCare Premium services and to register your device, please visit support.fortinet.com.

8.2 FortiGuard Unified Threat Protection (UTP)

The included 1 year of FortiGuard UTP provides real-time threat intelligence and security services, including:

- Antivirus and anti-malware protection
- Web filtering and URL blocking
- Intrusion Prevention System (IPS) updates
- Anti-spam and anti-botnet services

Ensure your FortiGate-60F is connected to the internet to receive the latest FortiGuard updates automatically.

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			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 8.1: Overview of FortiGuard and FortiCare subscription categories and service offerings.

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/B081268J3Q

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