FORTINET FGR-60F

FORTINET FortiGate Rugged 60F Network Security Appliance User Manual

Model: FGR-60F

1. Introduction

This manual provides essential information for the installation, operation, and maintenance of your FORTINET FortiGate Rugged 60F Network Security Appliance. The FortiGate Rugged 60F is designed to deliver robust network security in harsh industrial environments, offering advanced threat protection and secure SD-WAN capabilities.
It features a fanless design and robust components, ensuring reliable operation in challenging conditions, including those with high electrical and radio frequency interference, and wide ambient temperature ranges. The device runs on FortiOS, providing specialized protections for industrial networks.

2. Safety Information

Please read and understand all safety instructions before installing or operating the device. Failure to comply with these instructions may result in injury, damage to the device, or voiding of the warranty.

- **Electrical Safety:** Ensure the device is connected to a grounded power source. Do not operate with damaged power cords.
- **Environmental Conditions:** Operate the device within specified temperature and humidity ranges. Avoid exposure to direct sunlight, excessive heat, moisture, or corrosive substances.
- **Ventilation:** Although fanless, ensure adequate airflow around the device to prevent overheating.
- **Handling:** Handle the device with care. Avoid dropping or subjecting it to severe impacts.
- **Servicing:** Refer all servicing to qualified personnel. Do not attempt to open or repair the device yourself.

3. Package Contents

Verify that all items are present in your package:

- FORTINET FortiGate Rugged 60F Appliance (Base Unit)
- Power Adapter
- Documentation (Quick Start Guide, Safety Information)
- Mounting Hardware (if applicable for industrial installations)

4. Physical Overview

The FortiGate Rugged 60F features a compact, robust design with various ports and indicators on its front panel for connectivity and status monitoring.

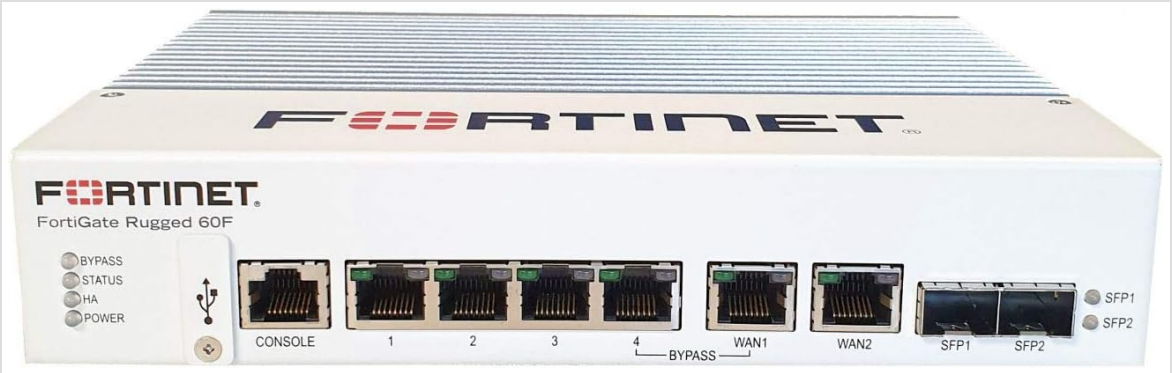


Image 4.1: Front panel of the FortiGate Rugged 60F. This image displays the console port, four LAN ports, two WAN ports, two SFP ports, a USB port, and LED indicators for BYPASS, STATUS, IHA, and POWER.

Front Panel Components:

- **Console Port:** RJ45 port for command-line interface (CLI) access.
- **LAN Ports (1-4):** Four Ethernet ports for connecting to internal networks.
- **WAN Ports (WAN1, WAN2):** Two Ethernet ports for connecting to external networks or the internet.
- **SFP Ports (SFP1, SFP2):** Two Small Form-Factor Pluggable ports for fiber or copper transceivers.
- **USB Port:** For connecting external devices or for firmware updates.
- **LED Indicators:**
  - **BYPASS:** Indicates bypass mode status.
  - **STATUS:** System status indicator.
  - **IHA:** Indicates High Availability status.
  - **POWER:** Power status indicator.

5. Setup

Follow these steps to set up your FortiGate Rugged 60F appliance.

5.1. Mounting

The FortiGate Rugged 60F is designed for industrial environments. Securely mount the device using appropriate hardware and methods suitable for your installation location. Ensure the mounting surface is stable and can support the device's weight.

5.2. Connecting Power

1. Connect the power adapter to the device's power input.
2. Plug the power adapter into a grounded electrical outlet.
3. Verify that the POWER LED indicator illuminates.

5.3. Network Connections

1. Connect your internet service provider's cable to one of the**WAN** ports.
2. Connect your internal network devices (e.g., switches, computers) to the**LAN** ports.
3. For initial configuration, you may connect a computer directly to the**Console** port using an RJ45-to-serial cable and a terminal emulator.

6. Operation

Once powered on and connected, the FortiGate Rugged 60F can be configured and managed through its FortiOS operating system.

6.1. Initial Access

Access the FortiGate device via a web browser or the command-line interface (CLI) through the console port. Refer to the FortiGate documentation for default IP addresses and login credentials.

6.2. FortiOS Configuration

FortiOS provides a comprehensive suite of security and networking features. Key configuration areas include:

- **Network Settings:** Configure interfaces, routing, and VLANs.
- **Security Policies:** Define rules for traffic flow and threat inspection.
- **Firewall:** Implement firewall rules to protect your network.
- **VPN:** Set up Virtual Private Networks for secure remote access or site-to-site connectivity.
- **Threat Protection:** Configure antivirus, intrusion prevention, and web filtering.

For detailed configuration instructions, consult the official Fortinet FortiOS documentation available on the Fortinet support website.

7. Maintenance

Regular maintenance ensures optimal performance and longevity of your FortiGate Rugged 60F.

- **Firmware Updates:** Regularly check for and apply the latest FortiOS firmware updates to ensure your device has the most current security features and bug fixes.
- **Configuration Backups:** Periodically back up your device configuration. This allows for quick restoration in case of an issue.
- **Environmental Monitoring:** Ensure the operating environment remains within specified temperature and humidity limits.
- **Physical Inspection:** Periodically inspect the device for any physical damage or loose connections.
- **Cleaning:** Keep the device free from dust and debris. Use a soft, dry cloth for cleaning. Do not use liquid cleaners.

8. Troubleshooting

This section provides solutions to common issues you might encounter.

8.1. LED Indicator Meanings

- **POWER LED Off:** No power. Check power cable connection and power outlet.
- **STATUS LED Red:** System error. Consult Fortinet documentation or support.
- **Link/Activity LEDs Off:** No network connection on that port. Check cable and connected device.

8.2. Common Issues

- **Cannot Access Web Interface:**
  - Ensure your computer is on the same network segment as the FortiGate's management interface.
  - Verify the correct IP address and port (e.g., HTTPS).
  - Try accessing via the console port CLI.
- **No Internet Connectivity:**
  - Check WAN port cable connection and ISP status.
  - Verify WAN interface configuration and routing policies in FortiOS.
  - Ensure DNS settings are correct.
- **Slow Performance:**
  - Check CPU and memory utilization in FortiOS.
  - Review security policies for potential bottlenecks.
  - Ensure firmware is up to date.

For more advanced troubleshooting, refer to the Fortinet support website or contact technical support.

9. Specifications

Technical specifications for the FORTINET FortiGate Rugged 60F (FGR-60F) Network Security Appliance:

Feature	Detail
Model Number	FGR-60F
Dimensions (H x W x L)	1.68 x 8.50 x 6.50 inches (42.7 x 216 x 165 mm)
Weight	3.85 lbs (1.75 kg)
IP Rating	IP20
IPv4 Firewall Throughput (1518/512/64 byte UDP)	6/6/5.95 Gbps
New Sessions/Second (TCP)	19,000
IPsec VPN Throughput (512 byte)	3.5 Gbps
IPS Throughput	950 Mbps
SSL-VPN Throughput	400 Mbps
Operating System	FortiOS
Security Protocols	WPA2, WPA3
Connectivity Technology	Ethernet
Special Feature	WPS
Manufacturer	Fortinet, Inc.
Date First Available	August 24, 2020

10. Warranty and Support

FORTINET provides various support services and security subscriptions to ensure the optimal performance and security of your FortiGate Rugged 60F.

10.1. FortiCare Support Services

FortiCare services offer technical support and hardware replacement options. Different tiers are available to meet various operational requirements.

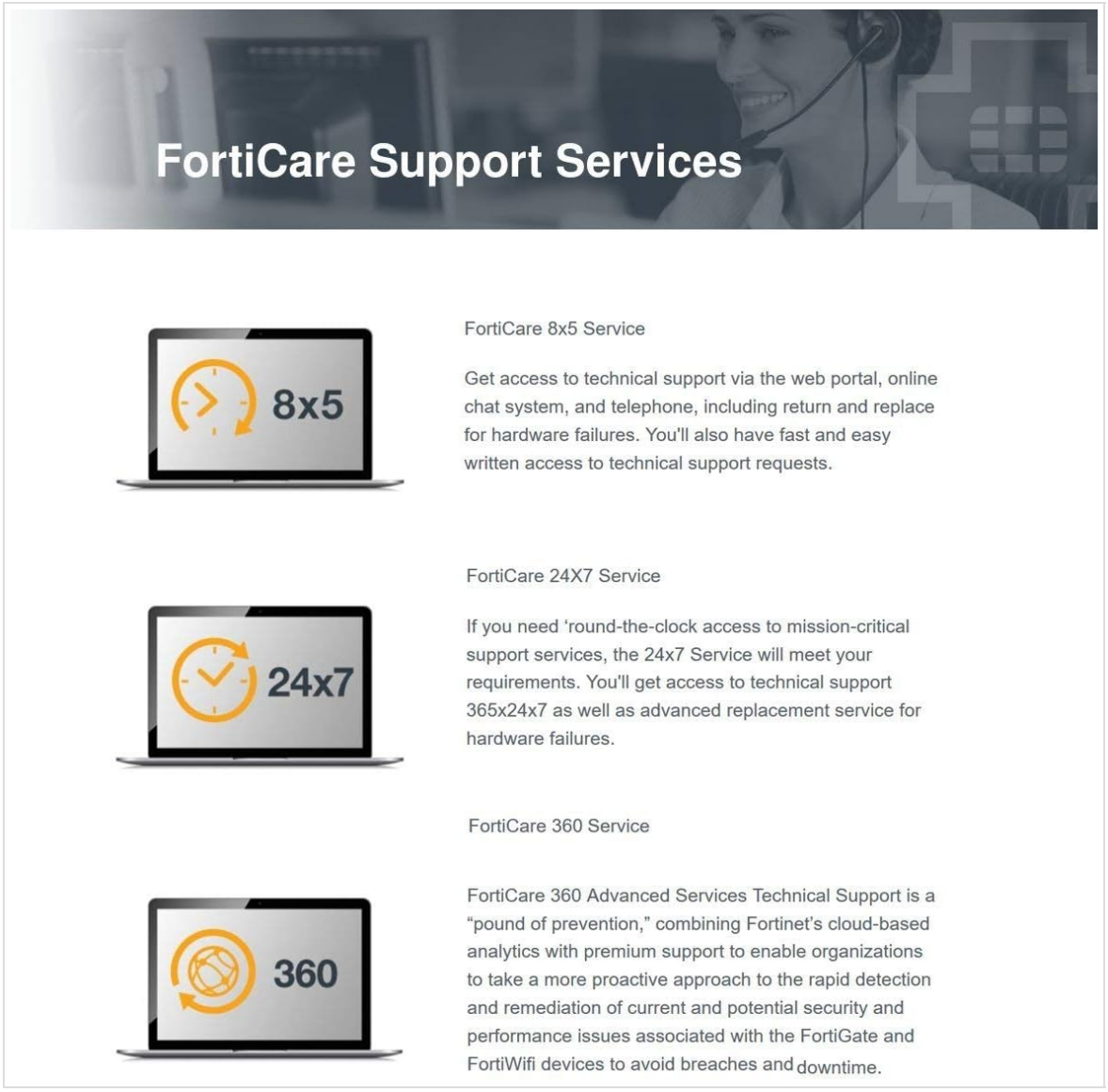


Image 10.1: FortiCare Support Services. This image details the 8x5, 24x7, and 360 service options, explaining their coverage for technical support, hardware replacement, and proactive analytics.

- **FortiCare 8x5 Service:** Provides access to technical support via web portal, online chat, and telephone, including return and replace for hardware failures.
- **FortiCare 24x7 Service:** Offers round-the-clock access to mission-critical support, including advanced replacement service for hardware failures.
- **FortiCare 360 Service:** Combines Fortinet's cloud-based analytics with premium support for proactive threat detection and remediation.

10.2. Security Subscriptions

Fortinet's security subscriptions, powered by FortiGuard Labs, provide real-time threat intelligence and protection against evolving cyber threats.

Image 10.2: Security Subscriptions. This image highlights the benefits of Fortinet's security subscriptions, including up-to-the-minute threat intelligence, global insight, comprehensive analytics, high fidelity processes, prevention of exploitation, and top-rated effectiveness.

FortiGuard Subscription Options

Here is a brief overview of the FortiGuard subscription feeds available for your organizations:

Next-Generation Application Control and IPS

Application control and intrusion prevention (IPS) are foundational security technologies for a Next-Generation Firewall like FortiGate. FortiGuard IPS blocks approximately 470,000 network intrusions, and new IPS signatures are being created and uploaded to deployed devices every single day.

Web Filtering

On any given day, FortiGuard Labs processes nearly 50 million URL categorization requests and blocks over 160,000 malicious websites. The FortiGuard Web Filtering service rates over 250 million websites and delivers nearly 1.5 million new URL ratings every week. Websites are categorized into six major categories for fast control, and nearly 80 micro-categories for fine-tuned control.

Antivirus

FortiGuard Labs has identified and neutralized nearly 100,000 malware programs targeting traditional, mobile, and IoT platforms. Patented technologies such as the Fortinet Content Pattern Recognition Language (CPRL) enable FortiGuard antivirus to identify thousands of current and future malware variants with a single signature – optimizing your deployment's security effectiveness and performance.

Web Application Security Service

The FortiWeb Security subscription service provides fully automated updates to protect your sensitive data and content from the latest application-layer threats. FortiGuard Labs provides updates on the latest advanced application vulnerabilities, bots, suspicious URL patterns, data-type patterns, and heuristic detection engines to enable FortiWeb Security-enabled appliances to prevent both new and evolving-application threats from gaining access to your web applications.

Antispam

Email is still the #1 vector for the start of an advanced attack on an organization, so a highly effective antispam solution should be a key part of any security strategy. FortiGuard Antispam detects unwanted and often malicious email with global spam filtering that uses sender IP reputation and spam signatures. To keep your antispam solution optimized, FortiGuard Labs delivers nearly 46 million new and updated spam rules every single week. The FortiGuard Antispam feed is available for both the FortiMail and FortiGate solutions.

Vulnerability Scan

The FortiGuard Vulnerability Scan service helps the FortiClient solution accurately identify and manage the latest software vulnerabilities on endpoint devices. It identifies the OS and applications, and discovers known vulnerabilities in versions of software currently running on the endpoints in your organization. It also provides timely remediation intelligence to help you remediate systems that have been identified as vulnerable.

Botnet IP and Domain Reputation

Every minute of every day, FortiGuard Labs blocks approximately 32,000 botnet command & control communication attempts. A key part of a botnet's attack kill chain requires an infected device to communicate with a command & control server – either to download additional threats or to exfiltrate stolen data. FortiGuard's IP and domain address reputation tools block this communication, thereby neutralizing these threats.

Database Security Control

FortiGuard's Database Security service offers centrally managed, enterprise-scale database protection for Fortinet's FortiDB product line. Automated content updates provide the latest pre-configured policies that cover known exploits, configuration weaknesses, OS issues, operational risks, data access privileges, and industry/regulatory best practices.

Mobile Security Service

Protect your organization against attacks targeting your mobile platforms. Fortinet's Mobile Security Service gives you the ability to create effective protection against the latest threats targeting mobile devices. It employs industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network and its invaluable content.

Advanced Threat Protection (FortiSandbox Cloud)

Thousands of organizations leverage FortiSandbox to identify advanced threats. FortiSandbox utilizes the full FortiGuard antivirus database, along with community reputation lookups, platform-independent code emulation, and virtual sandboxing to identify zero-day threats and attacks using new evasion tactics. The FortiSandbox Cloud service leverages this same FortiSandbox technology, and is integrated with the FortiGate platform.

Image 10.3: FortiGuard Subscription Options. This image provides a detailed overview of various FortiGuard services such as Next Generation Application Control and IPS, Antivirus, Antispam, Vulnerability Scan, Botnet IP and Reputation, Database Security Control, Mobile Security Service, and Advanced Threat Protection (FortiSandbox Cloud).

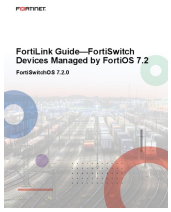
These subscriptions include services such as:

- Up-to-the-minute threat intelligence
- Antivirus and Intrusion Prevention
- Web Filtering and Antispam
- Vulnerability Scan and Botnet IP Reputation
- Advanced Threat Protection (FortiSandbox Cloud)

For more information on FortiCare services and security subscriptions, please visit the official Fortinet website or contact your Fortinet reseller.

Related Documents - FGR-60F

	FortiGate Ruggedized Accessories Datasheet Datasheet for FortiGate Ruggedized Accessories, focusing on the Industrial Strength DIN Rail Rugged Power Supply (SP-RGDIN-240-PS). Details include specifications, installation, engineering data, and ordering information.
	FortiOS 6.2.9 Release Notes This document provides release information for FortiOS version 6.2.9, detailing supported models, special notices, upgrade procedures, product integration, resolved issues, known issues, and limitations.
	FortiOS 6.4.3 Release Notes Official release notes for FortiOS version 6.4.3, detailing new features, enhancements, resolved issues, and known issues for Fortinet's network security operating system. Includes supported models and upgrade information.
	FortiGate Rugged 70G QuickStart Guide A quick start guide for the FortiGate Rugged 70G (FGR-70G), covering essential setup, package contents, power installation, wiring, grounding, dimensions, mounting, digital I/O connector, BIOS options, and regulatory information.

	[FortiLink Guide for FortiSwitch Devices Managed by FortiOS 7.2] This guide details the configuration and management of FortiSwitch devices using FortiOS 7.2 via FortiLink, covering network topologies, MCLAG, VLANs, STP, PoE, and security features for robust network infrastructure.
	[FortiOS 7.6.3 Release Notes - Fortinet] Detailed release notes for Fortinet FortiOS version 7.6.3, covering new features, resolved issues, known issues, upgrade information, and product integration for FortiGate devices.