manuals.plus /

› FORTINET /

› Fortinet FortiGate-101E Unified Threat Management Appliance User Manual

FORTINET FG-101E-BDL-950-12

Fortinet FortiGate-101E Unified Threat Management Appliance User Manual

Model: FG-101E-BDL-950-12

1. Introduction

The Fortinet FortiGate-101E is a unified threat management (UTM) appliance designed to provide comprehensive network security. This device integrates multiple security functions, including firewall, VPN, intrusion prevention, and content filtering, into a single platform. This manual provides instructions for the proper installation, configuration, and maintenance of your FortiGate-101E appliance.

2. Safety Information

- Always connect the appliance to a grounded power outlet.
- Ensure proper ventilation around the device to prevent overheating. Do not block ventilation openings.
- Do not expose the device to water or excessive humidity.
- Use only the power supply provided or specified by Fortinet.
- Refer all servicing to qualified service personnel.
- Before performing any maintenance, disconnect the power cable.

3. Package Contents

Verify that your package contains the following items:

- FortiGate-101E Appliance
- Power Cable
- Rackmount Kit (if applicable)
- Ethernet Cable
- Quick Start Guide

4. Hardware Overview

4.1 Front Panel

The front panel of the FortiGate-101E features various ports and LED indicators for status monitoring and connectivity.

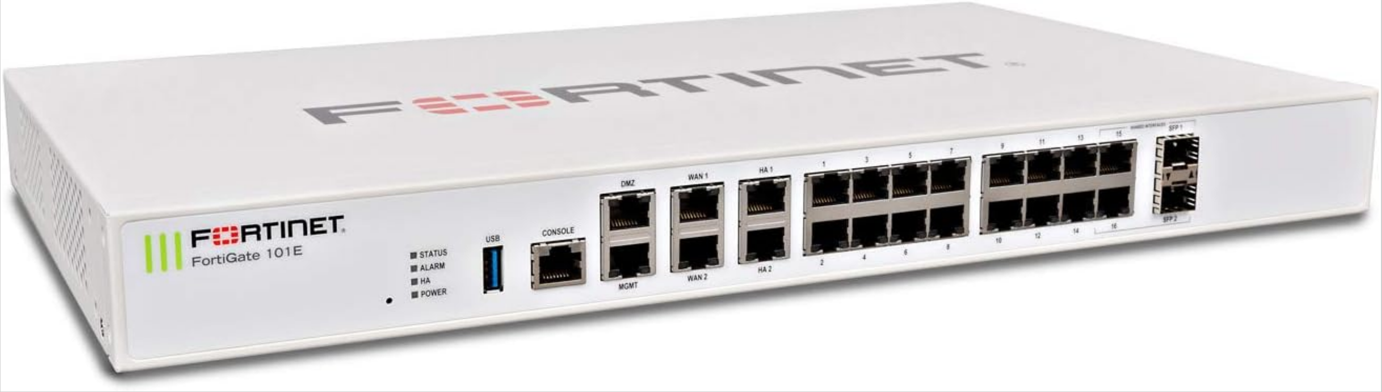


Figure 4.1: Front view of the FortiGate-101E appliance, showing the status LEDs, USB port, Console port, and various Ethernet and SFP ports for network connectivity.

- **Status LEDs:** Indicate power, system status, alarm, and HA (High Availability) status.
- **USB Port:** For connecting external storage or other USB devices.
- **Console Port:** RJ45 serial port for direct command-line interface (CLI) access.
- **Network Ports:** Multiple RJ45 Ethernet ports (WAN, HA, internal) and SFP ports for fiber optic connections.

4.2 Rear Panel

The rear panel includes the power input and additional ventilation.

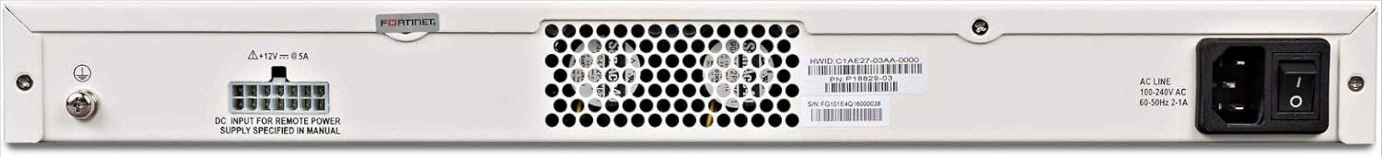


Figure 4.2: Rear view of the FortiGate-101E appliance, showing the AC power input, DC input for remote power supply, and ventilation grilles.

- **AC Power Input:** Standard IEC C14 power connector.
- **DC Input:** For remote power supply, as specified in the manual.
- **Ventilation:** Ensures proper airflow for cooling the internal components.

5. Setup

5.1 Physical Installation

The FortiGate-101E can be installed on a desktop or mounted in a standard 19-inch rack.

- **Desktop Installation:** Place the appliance on a flat, stable surface with adequate ventilation.
- **Rackmount Installation:** Attach the provided rackmount ears to the sides of the appliance using the screws. Secure the appliance into a standard 19-inch equipment rack.

5.2 Connecting Power

1. Connect the power cable to the AC power input on the rear panel of the FortiGate-101E.

2. Plug the other end of the power cable into a grounded electrical outlet.
3. The power LED on the front panel should illuminate.

5.3 Connecting Network Cables

Connect your network cables to the appropriate ports:

- **WAN Ports:** Connect to your internet service provider's modem or router.
- **Internal/LAN Ports:** Connect to your internal network switches or devices.
- **HA Ports:** For High Availability configurations, connect to another FortiGate appliance.
- **Management Port:** A dedicated port for initial configuration and management access.

5.4 Initial Configuration Access

To perform initial configuration, connect a computer to the FortiGate-101E:

- **Web-based Manager:** Connect an Ethernet cable from your computer to an internal or management port. Configure your computer's IP address to be in the same subnet as the FortiGate's default management IP (e.g., 192.168.1.99 for FortiGate 192.168.1.99). Open a web browser and navigate to the FortiGate's IP address.
- **Command Line Interface (CLI):** Connect a serial console cable from your computer's serial port to the FortiGate's Console port. Use a terminal emulator (e.g., PuTTY) with settings: 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control.

6. Operating Instructions

6.1 Basic Configuration

After initial access, you will need to configure basic network settings, including:

- Setting the administrator password.
- Configuring WAN interface IP address (DHCP or static).
- Defining internal network interfaces and DHCP servers.
- Creating firewall policies to allow traffic.

6.2 Firmware Updates

Regularly update the FortiGate firmware to ensure optimal performance and security. Firmware files can be downloaded from the Fortinet support website. Always back up your configuration before performing a firmware upgrade.

6.3 FortiGuard Services

The FortiGate-101E supports various FortiGuard security services to enhance protection. These services provide real-time threat intelligence updates.

FortiGuard Subscription Options

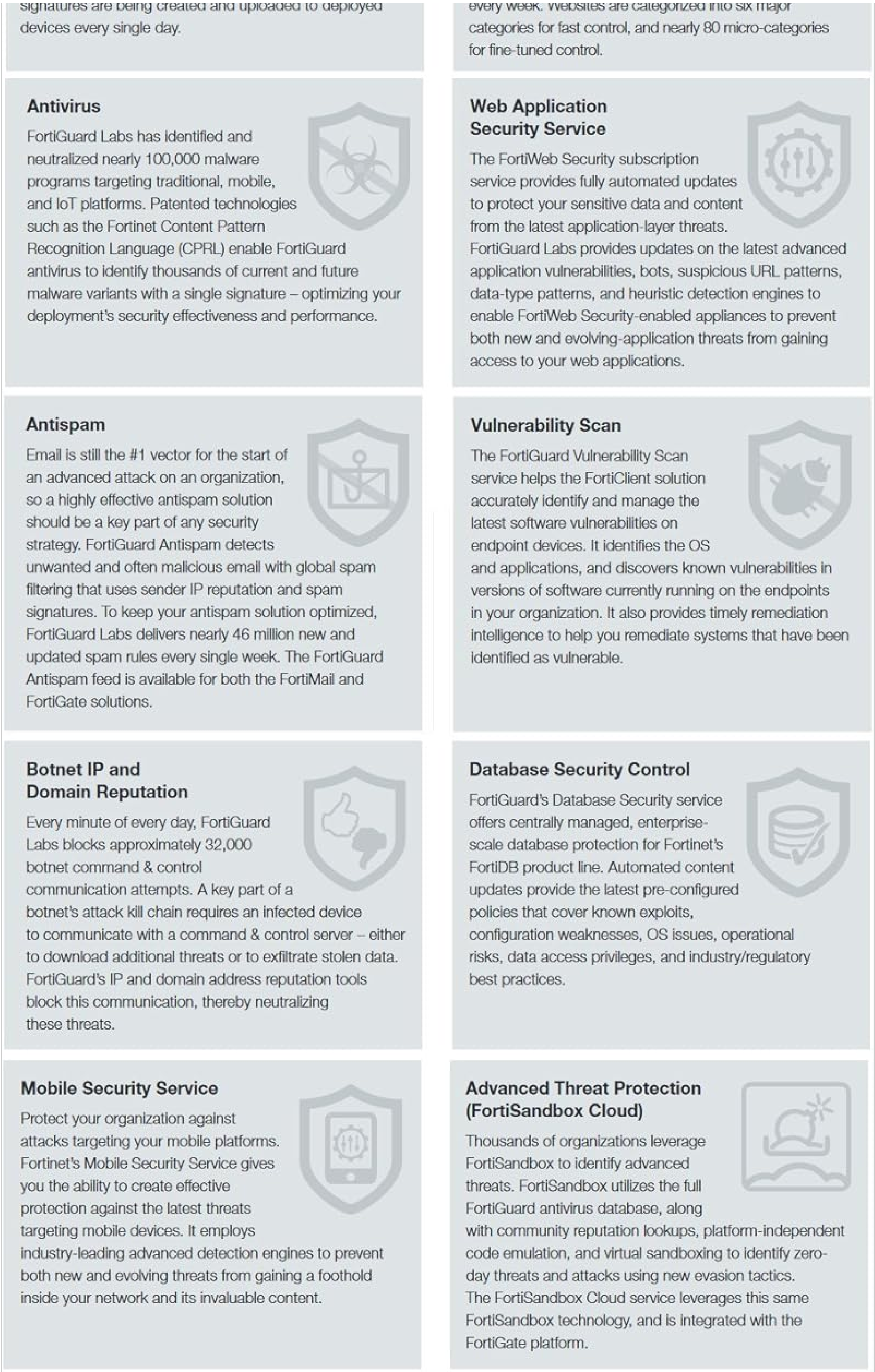
Here is a brief overview of the FortiGuard subscription feeds available for your organizations:

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

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



signatures are being created and uploaded to deployed devices every single day.

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.

Figure 6.1: Overview of FortiGuard subscription options, detailing services such as Next-Generation Application Control and IPS, Antivirus,

Web Application Security Service, Antispam, Vulnerability Scan, Botnet IP and Domain Reputation, Database Security Control, Mobile Security Service, and Advanced Threat Protection (FortiSandbox Cloud).

Key FortiGuard services include:

- **Next-Generation Application Control and IPS:** Identifies and blocks threats based on application and intrusion patterns.
- **Antivirus:** Detects and removes malware, ransomware, and other malicious software.
- **Web Filtering:** Blocks access to malicious or inappropriate websites.
- **Antispam:** Filters unwanted email and protects against phishing attempts.
- **Botnet IP and Domain Reputation:** Prevents communication with known malicious botnet infrastructure.

For detailed configuration of these services, refer to the FortiGate Administration Guide available on the Fortinet support website.

7. Maintenance

- **Regular Configuration Backup:** Periodically back up your FortiGate configuration to an external storage device or management server.
- **Monitor System Logs:** Regularly review system logs for any unusual activity or errors.
- **Keep Firmware Updated:** Ensure the device runs the latest stable firmware version.
- **Physical Cleaning:** Keep the appliance free from dust. Use a soft, dry cloth to clean the exterior. Do not use liquid cleaners.

8. Troubleshooting

8.1 Common Issues and Solutions

- **No Power:**
  - Check if the power cable is securely connected to both the appliance and the power outlet.
  - Verify the power outlet is functional.
  - Ensure the power LED on the front panel is illuminated.
- **No Network Connectivity:**
  - Check if Ethernet cables are properly connected to the correct ports.
  - Verify link/activity LEDs on the connected ports.
  - Ensure IP addresses and subnet masks are correctly configured on both the FortiGate and connected devices.
  - Check firewall policies to ensure traffic is allowed.
- **Cannot Access Web-based Manager:**
  - Ensure your computer's IP address is in the same subnet as the FortiGate's management IP.
  - Try clearing your browser's cache or using a different browser.
  - Attempt to access via CLI using the console port.

8.2 LED Indicators

Refer to the front panel LEDs for quick status checks:

- **Power LED:** Solid green indicates power is on.

- **Status LED:** Indicates system operational status (e.g., solid green for normal operation, blinking for activity).
- **Alarm LED:** Red indicates a system alarm or fault.
- **HA LED:** Indicates High Availability status (if configured).

9. Specifications

Feature	Detail
Model Number	FG-101E-BDL-950-12
Brand	FORTINET
Manufacturer	Fortinet
Product Dimensions	10 x 17.01 x 1.75 inches
Item Weight	7.28 pounds (3300 Grams)
Data Transfer Rate	4000 Megabits Per Second
Control Method	App (Web-based UI, CLI)
Special Feature	WPS (Note: Typically not used on enterprise firewalls)
Compatible Devices	Network devices, Servers, Workstations
ASIN	B06VSW8VBY
UPC	619587314198, 728350941148

10. Warranty and Support

For detailed warranty information, please refer to the official Fortinet website or the warranty card included with your product. Fortinet provides technical support and resources for its products.
Online Resources:

- Fortinet Support Portal: https://support.fortinet.com
- Documentation Library: https://docs.fortinet.com

It is recommended to register your product on the Fortinet support portal to access firmware updates, technical documentation, and support services.