FORTINET FG-201E-BDL-950-60

Fortinet FortiGate-201E Hardware User Manual

Comprehensive guide for the setup, operation, and maintenance of your FortiGate-201E Next-Generation Firewall.

1. Product Overview

The Fortinet FortiGate-201E is a high-performance next-generation firewall designed for mid-sized to large enterprises. It provides robust protection against cyber threats with security processor-powered capabilities, ensuring high performance, security efficacy, and deep visibility into network traffic. This device is suitable for deployment at campus or enterprise branch locations.

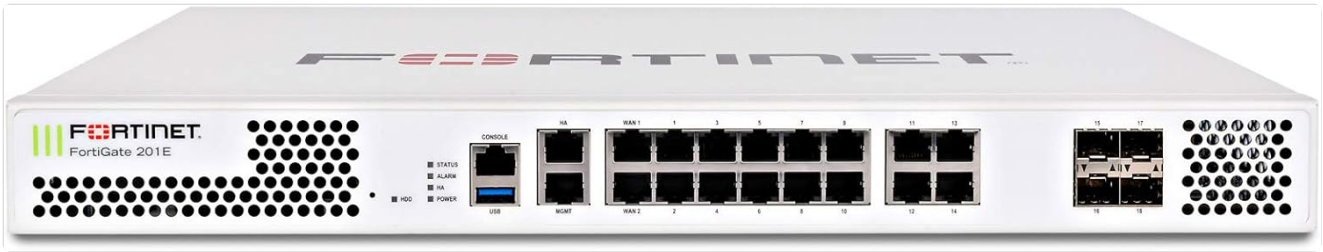


Figure 1: Front view of the Fortinet FortiGate-201E hardware unit.

This image displays the front panel of the FortiGate-201E, showing the Fortinet branding, model name, status indicators (STATUS, ALARM, HA, POWER), HDD activity light, USB port, console port, and various Ethernet and SFP+ ports for network connectivity.

2. Key Features

The FortiGate-201E offers a comprehensive suite of features to secure your network:

- **Next-Generation Firewall (NGFW) Capabilities:** Provides advanced threat protection, including intrusion prevention, application control, and web filtering.
- **Unified Threat Management (UTM):** Integrates multiple security functions such as antivirus, anti-spam, and botnet IP/domain protection.
- **High Performance:** Leverages security processors for accelerated threat detection and network throughput.
- **Extensive Port Connectivity:** Features multiple Ethernet and SFP+ ports for flexible network integration.
- **24x7 FortiCare and FortiGuard Protection:** Includes comprehensive support and real-time threat intelligence updates.

3. FortiGuard Services Overview

FortiGuard Services provide real-time threat intelligence and security updates to protect your FortiGate device. These services are crucial for maintaining an effective security posture.

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.

Figure 2: Overview of FortiGuard Subscription Options.

This diagram illustrates various FortiGuard services, including Next-Generation Application Control and Intrusion Prevention (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). Each service provides specific security benefits, such as protecting against exploits, malware, unwanted emails, and zero-day threats.

4. Specifications

Attribute	Value
Product Dimensions	11.85 x 17.01 x 1.73 inches
Item Weight	12.13 pounds
Manufacturer	FORTINET
ASIN	B06VT1RT92
Item Model Number	FG-201E-BDL-950-60
Date First Available	February 9, 2017
Brand	FORTINET
Model Name	Fortinet 9974712
Special Feature	WPS
Frequency Band Class	Dual-Band
Compatible Devices	Laptop
Recommended Uses For Product	Home
Connectivity Technology	Ethernet
Antenna Type	Internal
Security Protocol	WPS

5. Setup Guide

5.1 Unboxing and Initial Inspection

1. Carefully open the packaging and remove the FortiGate-201E unit and all accessories.
2. Verify that all components listed in the packing slip are present.
3. Inspect the unit for any signs of physical damage that may have occurred during shipping. If damage is found, contact your vendor immediately.

5.2 Physical Installation

The FortiGate-201E is designed for rack-mounting in a standard 19-inch equipment rack. Ensure adequate ventilation around the unit.

1. Choose a stable, level surface or a standard equipment rack for installation.
2. Ensure the installation location has proper environmental conditions (temperature, humidity) as specified in the product datasheet.
3. Mount the unit securely using the provided rack-mount ears and screws.
4. Connect the power cable to the AC inlet on the rear panel of the FortiGate unit and then to a grounded power outlet.
5. Connect network cables to the appropriate WAN and internal ports as per your network design. Refer to the port layout below.

Figure 3: Rear view of the Fortinet FortiGate-201E hardware unit.

This image shows the rear panel of the FortiGate-201E, highlighting the power input, grounding point, and ventilation fans. The label with model and serial number information is also visible.

6. Operating Instructions

6.1 Powering On

Once the unit is physically installed and connected, power it on:

1. Ensure the power cable is securely connected to both the FortiGate unit and a power outlet.
2. The unit will automatically power on. Observe the front panel LEDs. The POWER LED should illuminate green, and the STATUS LED should eventually turn green, indicating successful boot-up.

6.2 Initial Configuration

Initial configuration can be performed via the web-based manager or the command-line interface (CLI) through the console port.

- **Web-based Manager:** Connect a computer to one of the internal network ports (e.g., port 1) and configure your computer's IP address to be in the same subnet as the FortiGate's default management IP (typically 192.168.1.99). Open a web browser and navigate to https://192.168.1.99. Log in with the default username admin and no password.
- **CLI:** Connect a 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.

Note: *For detailed configuration steps, refer to the FortiGate Administration Guide available on the Fortinet support website.*

7. Maintenance

Regular maintenance ensures the optimal performance and longevity of your FortiGate-201E unit.

- **Firmware Updates:** Regularly check for and apply the latest firmware updates from Fortinet to ensure you have the most recent security patches and features.
- **Configuration Backups:** Periodically back up your FortiGate configuration. This is crucial for disaster recovery.
- **Monitor System Logs:** Review system logs regularly for any unusual activity or error messages.
- **Physical Inspection:** Ensure proper airflow around the unit. Keep vents clear of dust and obstructions.
- **FortiGuard Updates:** Verify that FortiGuard services are updating regularly to receive the latest threat intelligence.

8. Troubleshooting

This section provides solutions to common issues you might encounter.

Problem	Possible Cause	Solution
Unit does not power on.	No power, faulty power cable, or internal hardware issue.	Check power cable connection and outlet. Try a different power cable. If still no power, contact support.
Cannot access web-based manager.	Incorrect IP address, network connectivity issue, or browser problem.	Verify your computer's IP address is in the correct subnet. Check network cable connection. Try clearing browser cache or using a different browser.
Network traffic not flowing.	Incorrect port configuration, firewall policies blocking traffic, or cable issues.	Verify port assignments and cable connections. Check firewall policies and routes. Use diagnostic tools in the FortiGate CLI.
FortiGuard updates failing.	Network connectivity issues to FortiGuard servers, DNS resolution problems, or subscription expired.	Verify internet connectivity and DNS settings. Check FortiGuard subscription status. Ensure firewall policies allow FortiGuard traffic.

9. Warranty Information

The Fortinet FortiGate-201E hardware unit typically comes with a standard limited hardware warranty. The specific terms and duration of your warranty, including the 5-year 24x7 FortiCare and FortiGuard Unified (UTM) Protection bundle (FG-201E-BDL-950-60), are detailed in your purchase agreement and Fortinet's official warranty documentation.

For complete warranty details, please refer to the warranty statement provided with your product or visit the official Fortinet website.

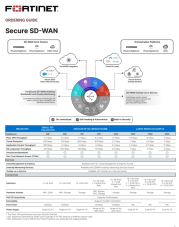
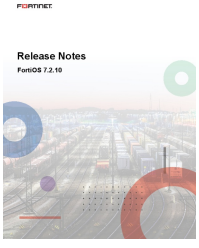
10. Support

For technical assistance, product documentation, and software downloads, please utilize the following resources:

- **Fortinet Support Website:** Visit support.fortinet.com for access to knowledge base articles, forums, and to open support tickets.
- **Fortinet Documentation Library:** Find comprehensive administration guides, installation guides, and release notes for your FortiGate model.
- **Fortinet Community:** Engage with other Fortinet users and experts for peer-to-peer support and best practices.

When contacting support, please have your product serial number (located on the unit's chassis) and a detailed description of your issue ready.

Related Documents - FG-201E-BDL-950-60

	[FortiOS 7.2.3 Release Notes - Fortinet] Official release notes for FortiOS version 7.2.3 by Fortinet, detailing new features, resolved issues, known issues, and upgrade information for FortiGate devices.
	[FortiOS 7.0.6 Release Notes - Fortinet] Comprehensive release notes for Fortinet FortiOS 7.0.6, detailing new features, resolved issues, known issues, and upgrade procedures for FortiGate network security devices.
	[Fortinet Secure SD-WAN Ordering Guide: Models, Bundles, and Specifications] This guide provides comprehensive ordering information for Fortinet's Secure SD-WAN solutions, detailing appliance models, performance specifications, bundle options, cloud integration, and management platforms for enterprise networks.
	[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.
	[FortiOS 7.6 AWS Administration Guide for Fortinet FortiGate-VM] Comprehensive guide to deploying and managing Fortinet FortiGate-VM instances on Amazon Web Services (AWS) with FortiOS 7.6, covering single deployments, HA, auto-scaling, and AWS service integration.
	[FortiOS 7.2.10 Release Notes - Fortinet] Explore the FortiOS 7.2.10 Release Notes from Fortinet. This document details new features, resolved issues, known issues, upgrade guidance, and supported models for FortiGate devices, enhancing network security and performance.