FORTINET FortiGate-200D

Fortinet FortiGate-200D Firewall Instruction Manual

Model: FortiGate-200D

1. PRODUCT OVERVIEW

The FortiGate 200D series provides high-speed security and performance for campus perimeter and branch office networks. It features purpose-built processors for up to 4 Gbps firewall throughput, ensuring protection without compromising availability or performance. This device includes comprehensive threat protection technologies such as firewall, VPN (IPsec and SSL), intrusion prevention, antivirus/antispyware, antispam, and web filtering. It also supports application control, data loss prevention, dynamic routing for IPv4 and IPv6, endpoint NAC, and SSL-encrypted traffic inspection. Onboard storage is included for local data archiving and web caching.

2. SETUP AND INSTALLATION

2.1 Unpacking and Inspection

Carefully unpack the FortiGate-200D unit and its accessories. Inspect all components for any signs of damage. If any damage is found, contact your vendor immediately.

2.2 Physical Installation

The FortiGate-200D is designed for rack-mounting. Ensure adequate ventilation around the unit to prevent overheating. Connect the power cable to the AC input on the rear panel and then to a grounded power outlet.

Image 2.2.1: Rear panel with AC input (100-240V, 50-60Hz, 3A Max) and power switch. Ensure the power switch is in the OFF position before connecting the power cable.

2.3 Network Connections

Connect network cables to the appropriate ports on the front panel. The FortiGate-200D features 18 GE RJ45 ports (16 x LAN, 2 x WAN) and 2 GE SFP DMZ ports.

- **WAN Ports:** Connect to your Internet Service Provider (ISP) or upstream network devices.
- **LAN Ports:** Connect to your internal network switches or devices.
- **DMZ Ports:** Connect to devices in your demilitarized zone, such as public-facing servers.
- **MGMT Port:** A dedicated management port for initial configuration and administration.
- **CONSOLE Port:** For direct console access using a serial cable.
- **USB MGMT Port:** For management via USB.

Image 2.3.1: Front panel of the FortiGate-200D, displaying the USB MGMT, MGMT, CONSOLE, STATUS, HA, ALARM, and POWER indicators, along with various RJ45 and SFP ports for network connectivity.

2.4 Initial Power On

After all connections are secure, switch the power button to the ON position. The device will begin its boot sequence. Monitor the status indicators on the front panel.

3. OPERATING INSTRUCTIONS

3.1 Accessing the Device

The FortiGate-200D can be accessed via a web-based graphical user interface (GUI) or through the command-line interface (CLI) via the console port or SSH.

- **GUI Access:** Open a web browser and enter the default IP address of the management interface (refer to the FortiGate documentation for the default IP).
- **CLI Access:** Connect a serial cable to the CONSOLE port and use a terminal emulator (e.g., PuTTY) with appropriate serial settings (e.g., 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control).

3.2 Basic Configuration

Upon first login, you will typically be prompted to change the default administrator password. Configure network interfaces, set up basic firewall policies, and enable necessary security features.

- **Network Interfaces:** Assign IP addresses, subnet masks, and default gateways to WAN, LAN, and DMZ interfaces.
- **Firewall Policies:** Create rules to control traffic flow between different network segments and to/from the

internet.

- **Security Profiles:** Enable and configure intrusion prevention, antivirus, web filtering, and application control profiles as required.

3.3 Advanced Features

The FortiGate-200D supports advanced features for enhanced security and network management:

- **VPN:** Configure IPsec or SSL VPNs for secure remote access or site-to-site connectivity.
- **Data Loss Prevention (DLP):** Implement policies to prevent sensitive data from leaving the network.
- **Dynamic Routing:** Utilize protocols like OSPF or BGP for complex network topologies.
- **Endpoint NAC:** Control network access based on endpoint security posture.

4. MAINTENANCE

4.1 Firmware Updates

Regularly check for and apply firmware updates to ensure your device has the latest features, security patches, and bug fixes. Firmware can be downloaded from the Fortinet support portal.

4.2 Configuration Backup and Restore

Periodically back up your device configuration. This allows for quick recovery in case of misconfiguration or hardware failure. Configuration files can be saved to a local computer or a remote server.

4.3 Monitoring and Logging

Monitor system logs and security events to detect potential threats or operational issues. The FortiGate-200D provides extensive logging capabilities, which can be viewed directly on the device or sent to a FortiAnalyzer or syslog server.

5. TROUBLESHOOTING

5.1 No Power

- Verify the power cable is securely connected to both the device and a working power outlet.
- Ensure the power switch on the rear panel is in the ON position.
- Check the power indicator LED on the front panel.

5.2 Network Connectivity Issues

- Check physical cable connections to the appropriate ports.
- Verify interface status in the GUI or CLI.
- Review firewall policies to ensure traffic is not being blocked unintentionally.
- Confirm IP address configurations and routing tables.

5.3 Performance Degradation

- Monitor CPU and memory utilization.
- Check for high session counts or excessive traffic.
- Review security logs for potential attacks or misconfigurations causing high load.
- Ensure firmware is up to date.

6. SPECIFICATIONS

Feature	Value
Model Number	FortiGate-200D
Data Transfer Rate	4 Gigabits Per Second
Number of Ports	18 (16 x LAN, 2 x WAN GE RJ45) + 2 GE SFP DMZ
Interface Type	RJ45, SFP
Voltage	100-240 Volts
Item Weight	17.26 pounds
Package Dimensions	22 x 20 x 7 inches
Onboard Storage	64GB onboard SDD
Hardware Acceleration	SPU NP4Lite and CP8 processors
UPC	619587330082

7. WARRANTY AND SUPPORT

7.1 Product Registration

To maximize the value of your FortiGate-200D and receive technical support, product updates, and protection from new threats, it is highly recommended to register your product. Registration details are typically found on a sticker or card included with the product, or can be completed on the official Fortinet website.

Image 7.1.1: Top view of the FortiGate-200D, showing a prominent "REGISTER" sticker with instructions to maximize product value and receive technical support.

7.2 Technical Support

For technical assistance, visit the official Fortinet support website. You will typically need your product's serial number and registration information to access support resources, documentation, and contact technical support personnel.

7.3 Warranty Information

Warranty terms and conditions for the FortiGate-200D are provided by Fortinet. Please refer to the warranty documentation included with your product or visit the Fortinet website for detailed information regarding warranty coverage and service procedures.