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

Fortinet FortiGate CLI Reference (FortiOS 3.0 MR7)

FortiGate CLI Reference Manual

Comprehensive Guide for FortiOS 3.0 MR7

Introduction

This document serves as a comprehensive reference for the FortiGate Command Line Interface (CLI). It details the syntax, usage, and functionality of all CLI commands available in FortiOS version 3.0 MR7. This manual is intended for network administrators and security professionals who manage FortiGate devices and require in-depth knowledge of CLI operations for configuration, monitoring, and troubleshooting.
The information contained herein was updated in January 2009 and corresponds to Fortinet document 01-30007-0015-20000112.



The image displays the cover of the FortiGate CLI Reference manual, featuring the Fortinet logo, the title 'FortiGate® CLI', and 'Version 3.0 MR7'.

Accessing the FortiGate CLI

The FortiGate CLI can be accessed through several methods:

- **Console Port:** Direct connection using a serial cable to the FortiGate device's console port. This method is essential for initial setup or recovery.
- **SSH (Secure Shell):** Remote access over a network using an SSH client. This requires the FortiGate device to have an IP address and SSH service enabled on an interface.
- **Telnet:** Remote access over a network using a Telnet client. Telnet is less secure than SSH and should be used with caution, preferably only on trusted internal networks.
- **Web-based Manager (GUI) CLI Console:** Many FortiGate models include a built-in CLI console accessible directly from the web-based graphical user interface.

Upon successful connection, you will be prompted for a username and password. Default credentials should be changed immediately after initial setup for security purposes.

Operating with CLI Commands

The FortiGate CLI follows a hierarchical command structure. Commands are organized into various configuration modes, such as global configuration, interface configuration, firewall policy configuration, etc.

Command Syntax and Navigation

Commands typically begin with a keyword followed by parameters. Context-sensitive help is available by typing a question mark (**?**) at any point in the command line. Pressing the Tab key can auto-complete commands or display available options.

- config system interface: Enters the interface configuration mode.
- edit port1: Selects 'port1' within the interface configuration mode.
- set ip 192.168.1.99 255.255.255.0: Sets the IP address for the selected interface.
- end: Exits the current configuration mode and saves changes.

Commonly Used Commands

Basic CLI Commands

Command	Description
get system status	Displays general system information, including firmware version, serial number, and uptime.
show full-configuration	Shows the complete running configuration of the FortiGate device.
execute ping <IP_address>	Sends ICMP echo requests to test network connectivity.
execute reboot	Reboots the FortiGate device. Requires confirmation.

Maintenance Operations via CLI

The CLI is a powerful tool for routine maintenance and system health checks.

- **Firmware Upgrades:** While often done via GUI, CLI commands can initiate firmware upgrades from a TFTP server.
- **Configuration Backup and Restore:** Save the current configuration to an external server or restore a previous configuration.

    - execute backup config tftp <filename> <tftp_server_ip>
    - execute restore config tftp <filename> <tftp_server_ip>
- **System Monitoring:** Commands like get system performance status or diagnose sys top provide real-time insights into CPU, memory, and session usage.

Troubleshooting with CLI

The CLI offers advanced diagnostic tools crucial for identifying and resolving network and device issues.

- **Packet Capture:** Use diagnose sniffer packet to capture and analyze network traffic passing through the FortiGate. This is invaluable for diagnosing connectivity or policy issues.
- **Debug Flow:** The diagnose debug flow command provides a detailed step-by-step trace of how a packet is processed by the FortiGate, helping to pinpoint where traffic is being dropped or misrouted.
- **Log Viewing:** Access system, traffic, and event logs directly from the CLI to review historical data for anomalies or errors.
- **Routing Table Inspection:** Commands like get router info routing-table all help verify routing paths and identify routing problems.

Specifications

This FortiGate CLI Reference manual specifically covers the Command Line Interface for FortiOS version 3.0 MR7. While many commands and concepts remain consistent across FortiOS versions, users should consult the official documentation for their specific FortiOS version for the most accurate and up-to-date information.

Document Title: FortiGate CLI Reference

Applicable FortiOS Version: 3.0 MR7

Publication Date: January 12, 2009

Publisher: Fortinet Technologies Inc.

Document ID: 01-30007-0015-20000112

Print Length: 726 pages

Support and Resources

For further assistance, technical support, product updates, and FortiGuard services, please refer to the official Fortinet support channels.

- **Fortinet Support Website:** http://support.fortinet.com
- **Product Registration:** Register your FortiGate CLI product on the support website to receive updates and access technical support.
- **Fortinet Documentation Library:** Access the latest documentation for all Fortinet products and FortiOS versions.
- **Fortinet Community Forums:** Engage with other Fortinet users and experts for peer-to-peer support and discussions.

Note: This manual provides a reference for a specific FortiOS version. Always consult the most current documentation available on the Fortinet support website for the latest features and security updates.

© 2009 Fortinet Technologies Inc. All rights reserved.
For more information, visit www.fortinet.com

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/B005D2RS4G

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