

FortiGate Lab: Security Fundamentals

This lab provides a hands-on learning experience with FortiGate firewalls. You'll explore key security features, network configurations, and best practices.

Objective of the Lab

1 Accessing the FortiGate CLI

You'll learn to connect to the FortiGate command-line interface (CLI) and navigate its commands.

2 Backing Up and Restoring

This section explores how to create backups and restore configuration files for disaster recovery and configuration management.

5

3 Model and Firmware

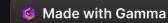
You'll practice locating and interpreting the FortiGate model and FortiOS firmware version from the configuration file.

4 Creating a User

This involves creating a new administrator user account with appropriate permissions and roles.

Restricting Access

You'll learn how to set up access restrictions and control permissions for administrators to enhance security.





Accessing the FortiGate CLI

SSH Connection

Establish a secure SSH connection to the FortiGate device using a terminal emulator like Putty.

Authentication

Login with your credentials: admin/admin or the credentials of the designated user.

Command Prompt

You'll be presented with the FortiGate CLI, allowing you to execute commands and manage the device.

Backing Up and Restoring Configuration Files

Backup

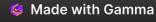
Use the 'get system config' command to generate a configuration file that contains the device settings.

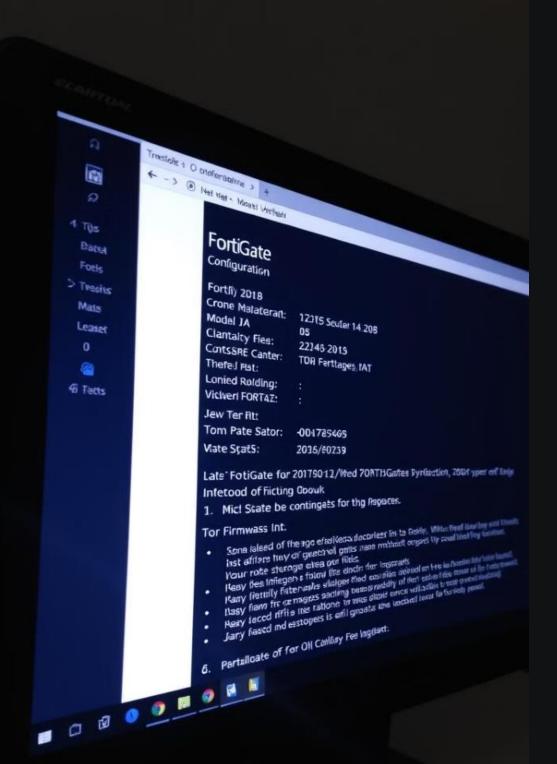
Save

Save the configuration file to a secure location, like a USB drive, for safekeeping.

Restore

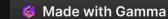
Utilize the 'config system from-file' command to load the configuration file back onto the FortiGate device.



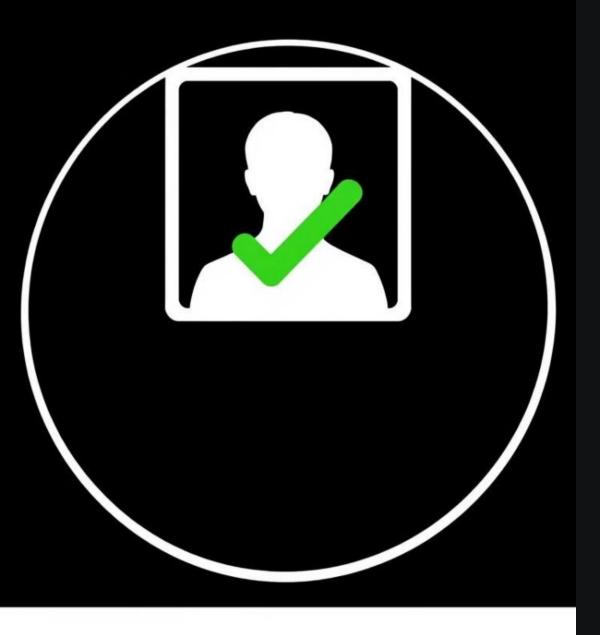


Locating the FortiGate Model and FortiOS Firmware Build

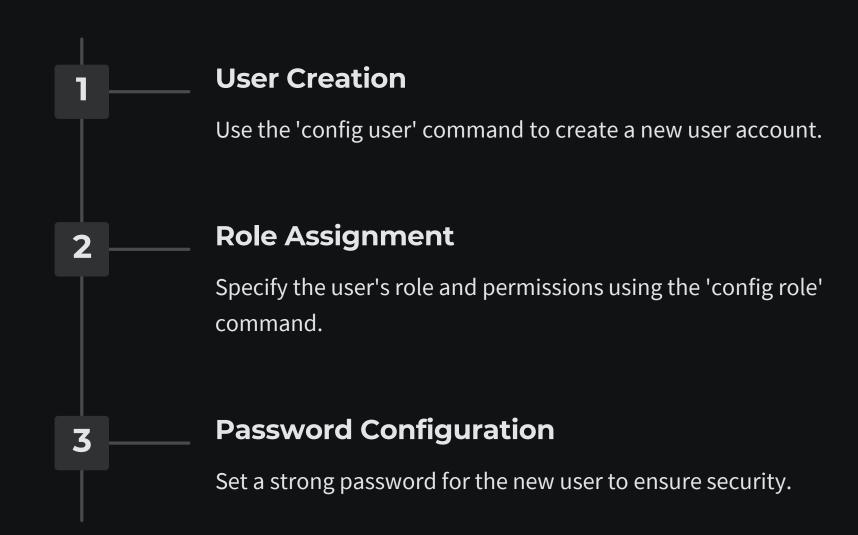
Command	Information
get system status	Model, serial number, hardware revision
get system version	FortiOS version, build number, and release date

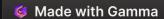


Newl Created



Creating a New Administrator User





Restricting Administrator Access



Access Control Lists (ACLs)

Use ACLs to restrict access to specific network resources based on IP addresses, ports, and protocols.



Firewall Policies

Configure firewall policies to control traffic flow and block unauthorized access based on defined rules.



User Roles

Assign granular permissions to different user roles to control the actions they can perform on the FortiGate device.





Lab Setup

Local-Client VM

Represents a user or device within the internal network, interacting with the FortiGate.

Local-FortiGate VM

The primary FortiGate device in the lab, acting as a firewall and security gateway.

Remote-Client VM

Represents a user or device outside the internal network, attempting to access resources.

Remote-FortiGate VM

An optional FortiGate device in the lab, demonstrating advanced security configurations and interdevice communication.

