Objective of the Lab

- Learn FortiGate administration using CLI and GUI.
- Back up and restore configuration files.
- Create and manage administrator accounts.
- Modify and test administrator access permissions.

Topology

- A virtualized setup including:
- - Local-Client VM
- - Remote-Client VM
- - Local-FortiGate
- - Remote-FortiGate
- - FortiAnalyzer
- - Subnet IP ranges for testing administrator access.

Components Used

- 1. FortiGate devices (Local and Remote).
- 2. FortiAnalyzer.
- 3. Local and Remote client machines with CLI and GUI access.
- 4. Software tools:
- - Mozilla Firefox for GUI operations.
- - Notepad++ for comparing configuration files.

Steps of the Lab

- 1. Explore the CLI:
- - Log in to the Local-FortiGate CLI.
- - Use basic commands like 'get system status' and shortcuts.
- - View configurations using commands like 'show system interface port3'.
- 2. Backup and Restore Configurations:
- - Back up the current configuration (plain text and encrypted).
- - Restore configurations from the saved

Testing the Lab

- - Log in using the new admin account to verify restricted access.
- - Test from both trusted and non-trusted subnets to confirm access limitations.
- - Validate the restored configuration by checking network interfaces and static routes.

Results

- 1. Successfully accessed FortiGate using CLI commands and GUI.
- 2. Backed up and restored configurations (both plain text and encrypted).
- 3. Created and verified an admin profile with restricted access.
- 4. Tested and confirmed restricted access based on trusted subnets.

Configuration Performed

- CLI Commands:
- # Display system status
- get system status

- # Show interface configuration
- show system interface port3

- # Add trusted subnet for admin account
- config system admin