Lab 1: FortiGate Introduction

Objective of the Lab

The main objectives of this lab are:

1. Accessing the FortiGate CLI.
2. Backing up and restoring configuration files.
3. Locating the FortiGate model and FortiOS firmware build in a configuration file.
4. Creating a new administrator user.
5. Restricting administrator access.

Topology

The lab setup involves multiple Virtual Machines (VMs) that interact with FortiGate devices and security systems:

- **Local-Client VM**
- **Remote-Client VM**
- **Local-FortiGate VM**
- **Remote-FortiGate VM**
- **ISFW VM**
- **FortiAnalyzer VM**

Components Used

1. **FortiGate firewall devices** (Local-FortiGate and Remote-FortiGate).
2. **Virtual Machines** for local and remote clients.
3. **FortiAnalyzer** for network analysis and security monitoring.
4. **Administrative access credentials** for testing configurations and security settings.

Steps of the Lab

1. Accessing the CLI:

- Log in to the Local-FortiGate CLI using the `admin` username and `password`.
- Use the command `get system status` to check system status. This will display information like the serial number, operating mode, and other basic details of the FortiGate device.

Commands used:

- `get system status`
  - Displays basic system information about the FortiGate device.
- `get ?`
  - Lists all available options after the `get` command.
- `show system interface port3`

    - Displays the configuration of the `port3` interface.
- `show full-configuration system interface port3`
    - Shows the full configuration of the `port3` interface, including default values.

2. Generating Configuration Backups:

- Log in to the Local-FortiGate GUI.
- Navigate to **Configuration > Backup** to generate both cleartext and encrypted configuration backups.
- Choose to either save the backup file locally or upload it for restoration later.

Commands used:

- Navigate in the GUI to **Configuration > Backup**.
- Select **Save File** or **Upload** based on your backup requirements.

3. Restoring Configuration from Backup:

- After generating the backup, log in to the Local-FortiGate GUI.
- Navigate to **Configuration > Restore**.
- Upload the previously saved backup file (either encrypted or cleartext).
- The system will reboot automatically after the restoration process.

Commands used:

- **Restore System Configuration**
    - Select the backup file and upload it to restore the configuration.

4. Configuring Administrator Accounts:

- Create a new administrator profile with specific permissions (e.g., read-only access to most configuration settings).
- After creating the profile, assign it to a new administrator account.

Commands used:

- **System > Admin Profiles**
    - Create a new administrator profile with read-only permissions for most configurations.
- **System > Administrators**
    - Create a new administrator account (e.g., `Security`) and assign it the created profile.

5. Restricting Administrator Access:

- Restrict access for administrators by setting allowed subnets or trusted IP addresses.
- This helps prevent unauthorized access to the FortiGate system.

Commands used:

- **System > Administrators**
  - Edit the administrator account (`Security`) and enable **Restrict login to trusted hosts**.
  - Set the trusted host subnet (e.g., `10.200.3.0/24`).
- Test the login by attempting access from an untrusted IP address.

Testing the Lab

- **CLI Access Testing:**
  - Use commands like `get system status` and `show system interface` to check system configurations.
  - Test various CLI shortcuts and commands to familiarize yourself with the FortiGate system.
- **Backup and Restore Testing:**
  - Test both encrypted and cleartext backup processes.
  - Verify that after restoring the configuration, network interfaces and static routes are properly restored.
- **Administrator Account Testing:**
  - Test the newly created administrator account (`Security`) to verify that it has limited access (read-only for most configurations).
  - Log in to the GUI using the `Security` account and ensure it cannot access restricted settings.
- **Access Restriction Testing:**
  - Test the restricted login feature by attempting to log in from an unauthorized subnet.
  - After applying the restriction, attempt a login from an authorized subnet to verify that access is allowed.

The Results

- **CLI and GUI Access:**
  - Successfully accessed the FortiGate CLI and GUI and confirmed that commands to view system status and interface configurations worked properly.
- **Backup and Restore:**
  - Configuration backups were successfully generated and restored. The system reverted to the previous configuration after a reboot.
- **Administrator Account Configuration:**
  - A new administrator account (`Security`) was created with read-only access for most configuration settings. Verified by logging in and checking available permissions.
- **Access Restrictions:**
  - Successfully restricted the `Security` administrator's access based on the trusted host IP subnet (`10.200.3.0/24`). Unauthorized login attempts were blocked, while authorized subnet access was allowed.

Configuration Done on Devices

CLI Commands:

1. `get system status`
   - Displays basic system information about the FortiGate device.
2. `show system interface port3`
   - Displays the configuration for the `port3` interface.
3. `show full-configuration system interface port3`
   - Displays the full configuration of the `port3` interface, including default values.

Backup and Restore:

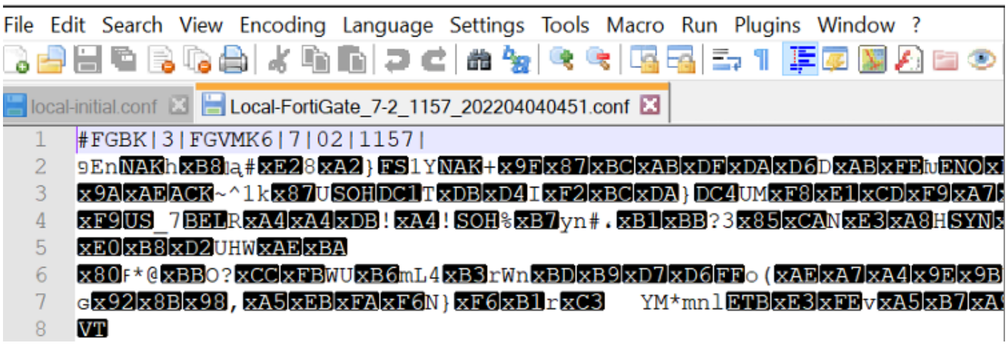
1. **Backup Configuration:**
   - GUI: **Configuration** > **Backup** (Cleartext and encrypted backup options).
2. **Restore Configuration:**
   - GUI: **Configuration** > **Restore** (Upload and restore from backup).

Administrator Configuration:

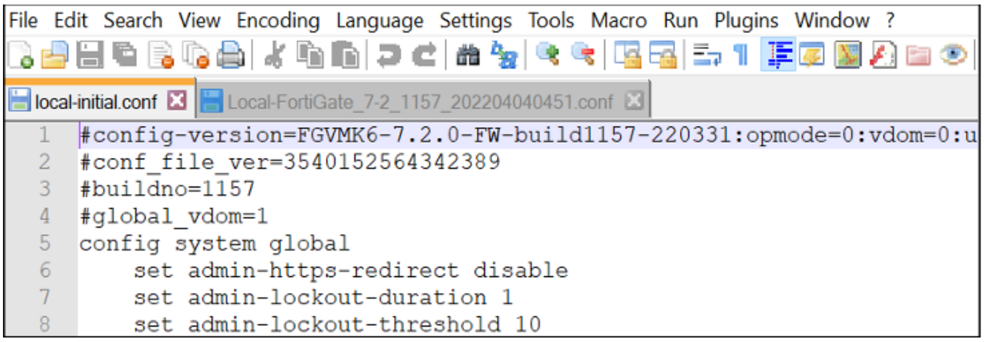
1. **Admin Profile Creation:**
   - GUI: **System** > **Admin Profiles** (Create new profile with limited permissions).
2. **Admin Account Creation:**
   - GUI: **System** > **Administrators** (Create `Security` account with assigned profile).

Access Restriction:

1. **Restrict Access by Subnet:**
   - GUI: **System** > **Administrators** (Set trusted IP subnet for admin account)


File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
local-initial.conf
Local-FortiGate_7-2_1157_202204040451.conf

```
#FGBK|3|FGVMK6|7|02|1157|
9EnNAKhxB8ą#xE28xA2}FS1YNAK+x9Fx87xBCxABxDFxDAxD6DxABxFEuENOx
x9AxAEACK~^1kx87USOHDC1TxDBxD4IxF2xBCxDA}DC4UMxF8xE1xCDxF9xA7
xF9US_7BELRxA4xA4xDB!xA4!SOH%xB7yn#.xB1xBB?3x85xCANxE3xA8HSYN
xE0xB8xD2UHWxAExBA
x80F*@xBBO?xCCxFBWUxB6mL4xB3rWnxBDxB9xD7xD6FFo(xAExA7xA4x9Ex9B
Gx92x8Bx98,xA5xEBxFAxF6N}xF6xB1rxC3    YM*mnlETBxE3xFEvxA5xB7xA
VT
```


File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
local-initial.conf
Local-FortiGate_7-2_1157_202204040451.conf

```
#config-version=FGVMK6-7.2.0-FW-build1157-220331:opmode=0:vdom=0:u
#conf_file_ver=3540152564342389
#buildno=1157
#global_vdom=1
config system global
    set admin-https-redirect disable
    set admin-lockout-duration 1
    set admin-lockout-threshold 10
```