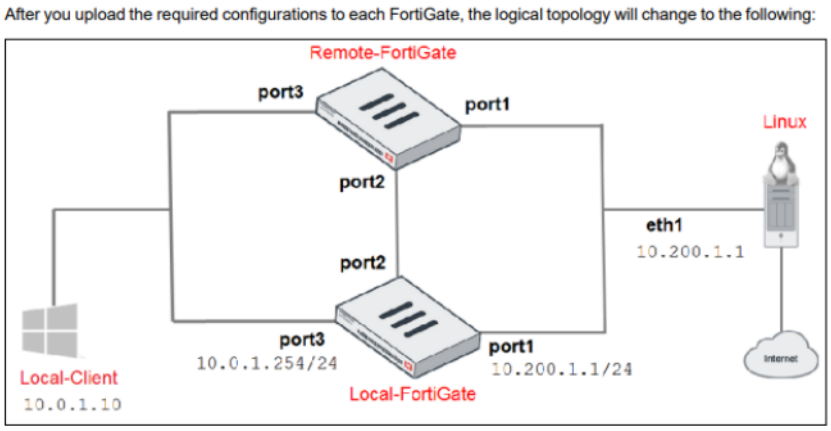
Fortinet Cybersecurity Lab: High Availability (HA) Setup

Objective

To explore the functionality of FGCP HA clustering in active-active mode, including:
1. Setting up an HA cluster.
2. Observing HA synchronization.
3. Performing HA failover.
4. Configuring reserved management interfaces for individual management of cluster members.

Topology



The topology consists of:
- Two FortiGate devices (one as Local, one as Remote).
- Linux server.
- Local Windows machine.
- A lab environment such as the Fortinet Portal.

Components Used

1. Two FortiGate devices (Local and Remote).
2. Supporting infrastructure:
   - A Linux server.
   - A local Windows machine for management and testing.
3. Fortinet lab environment.

Steps of the Lab

Part 1: Initial Configuration

1. Local FortiGate Setup:
   - Access Local FortiGate GUI using admin credentials.
   - Revert to the configuration labeled local-ha under Configuration > Revisions.
   - Reboot the device.

2. Remote FortiGate Setup:
   - Access Remote FortiGate GUI with admin credentials.
   - Revert to the configuration labeled initial under Configuration > Revisions.
   - Reboot the device.

3. HA Configuration on Local FortiGate:
   - Access Local FortiGate GUI.
   - Navigate to System > HA and configure HA settings.

4. HA Configuration on Remote FortiGate CLI:
   - Use the CLI to apply the following commands:

```
config system ha
set group-name Training
set mode a-a
set password Fortinet
set hbdev port2 0
set session-pickup enable
set override disable
set priority 100
end
```

Part 2: Testing and Observing HA Synchronization

1. Verify HA Synchronization:
   - Observe debug messages on the Remote FortiGate CLI to monitor the synchronization process.
   - Verify checksums match using:
     diagnose sys ha checksum show

2. Confirm Cluster Member Roles:
   - Check the HA status:
     get system ha status
   - Ensure the Local FortiGate is primary and Remote FortiGate is secondary.

Results

Test 1: Primary and Secondary Role Verification

- Confirm that the Local FortiGate was elected as the primary due to its higher priority.

Test 2: Failover

1. Initiate a failover by rebooting the Local FortiGate:
   execute reboot

2. Verify:
   - Traffic seamlessly continues through the Remote FortiGate, which assumes the primary role.
   - Ping and video streaming are unaffected during the failover.

3. Use the CLI command on Remote FortiGate to confirm its new role:
   get system ha status

Conclusion

This lab demonstrates the functionality of FortiGate's HA active-active mode, highlighting seamless traffic failover and management capability.