DEPI Graduation Project

Name: Khaled Osama Abdelmonem Mohamed

Track: Fortinet CyberSecurity Engineer

Student ID: 21037803

Group ID: CAI1_ISS8_S1e

Project: High Availability

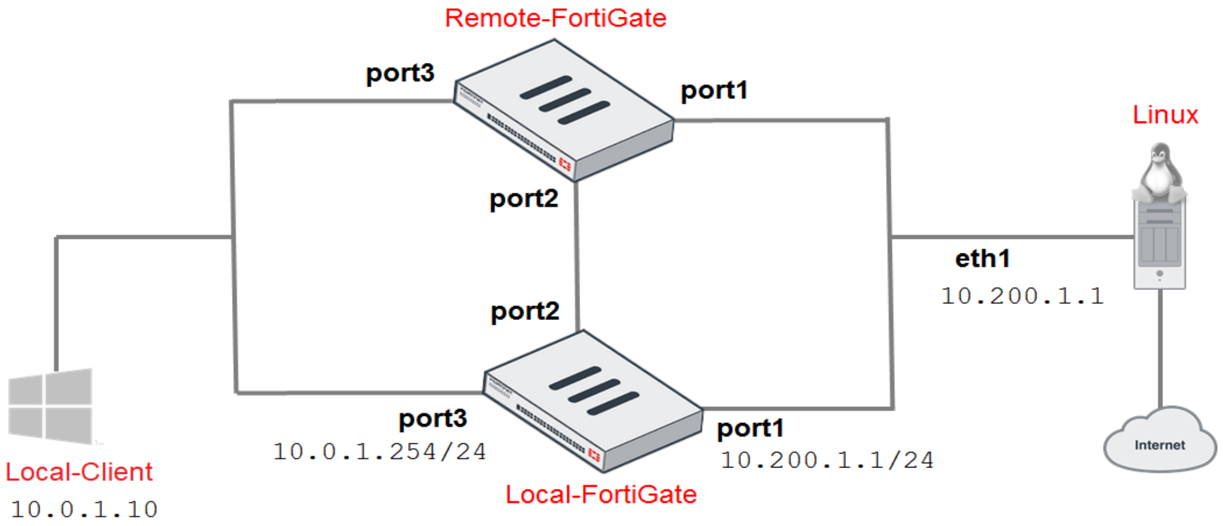
High Availability

In this lab, you will examine how to set up a FortiGate Clustering Protocol (FGCP) high availability (HA) cluster of FortiGate devices. You will explore active-passive HA mode and observe FortiGate HA behavior. You will also perform an HA failover and use diagnostic commands to observe the election of a new primary device in the cluster. Finally, you will configure management ports on FortiGate devices to reach each FortiGate individual for management purposes.

Objectives

- Set up an HA cluster using FortiGate devices
- Observe HA synchronization and interpret diagnostic output
- Perform an HA failover
- Manage individual cluster members by configuring a reserved management interface

Lab HA Topology



Exercise 1: Configuring HA

FortiGate HA uses FGCP, which uses a heartbeat link for HA-related communications to discover other FortiGate devices in the same HA group, elect a primary device, synchronize configuration, and detect failed devices in an HA cluster.

In this exercise, you will examine how to configure HA settings on both FortiGate devices. You will observe the HA synchronization status, and use diagnose commands to verify that the configuration is in sync on both FortiGate devices.

Configure HA Settings on Local-FortiGate

You will configure HA-related settings using the Local-FortiGate GUI.

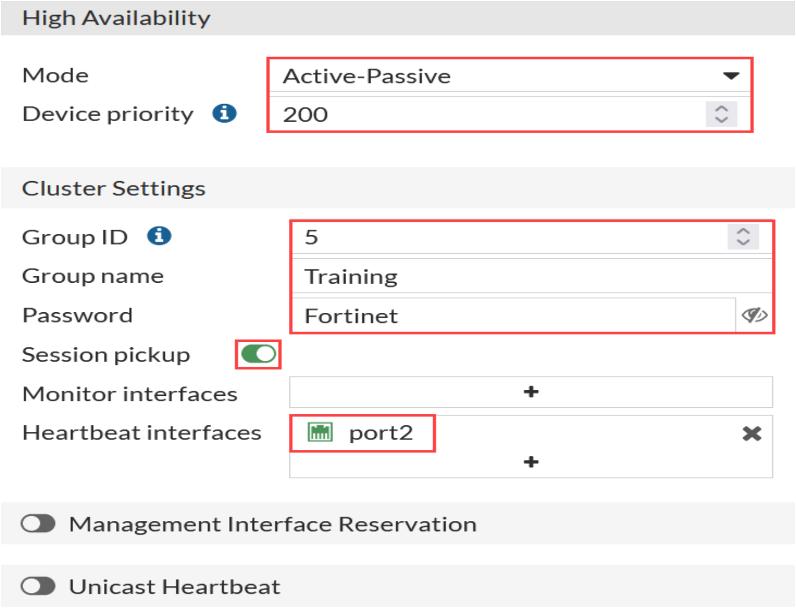
To configure HA settings on Local-FortiGate

1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password.
2. Click **System** > **HA**, and then configure the following HA settings:

Field	**Value**
Mode	Active-Passive
Device priority	200
Group ID	5
Group name	Training
Password	Fortinet **Tip**: Click **Change**, and then type the password.
Session pickup	<enable>

Field	**Value**
Monitor interfaces	Click **X** to remove any ports that are selected.
Heartbeat interfaces	Click **X** to remove port4, and then select port2.

The configuration should look like the following example:



High Availability

Mode: Active-Passive

Device priority: 200

Cluster Settings

Group ID: 5

Group name: Training

Password: Fortinet

Session pickup: enabled

Monitor interfaces:

Heartbeat interfaces: port2

Management Interface Reservation

Unicast Heartbeat

3. Click **OK**.

Configure HA Settings on Remote-FortiGate

You will configure HA-related settings on Remote-FortiGate, using the console.

To configure HA settings on Remote-FortiGate

1. Connect to the Remote-FortiGate CLI, and then log in with the username admin and password.
2. Enter the following commands:

   ```
   config system ha

   set mode a-p

   set group-name Training

   set group-id 5

   set password Fortinet

   set hbdev port2 0

   set session-pickup enable

   set override disable

   set priority 100

   end
   ```

Observe and Verify the HA Synchronization Status

Now that you have configured HA on both FortiGate devices, you will verify that HA is established and that the configurations are fully synchronized.

The checksums for all cluster members must match for the FortiGate devices to be synchronized.

To observe and verify the HA synchronization status

1. On the Remote-FortiGate CLI, notice the debug messages about the HA synchronization process.

   These messages sometimes display useful status change information.

2. Wait 4–5 minutes for the FortiGate devices to synchronize.

   After the FortiGate devices are synchronized, the Remote-FortiGate device logs out all admin users.

   ```
   secondary succeeded to sync external files with primary

   secondary starts to sync with primary

   logout all admin users
   ```

3. When prompted, log back in to the Remote-FortiGate CLI with the username admin and password password.

4. Enter the following command to check the HA synchronization status:

   ```
   diagnose sys ha checksum show
   ```

5. On the Local-FortiGate CLI, enter the following command to check the HA synchronization status:

   ```
   diagnose sys ha checksum show
   ```

6. Compare the output from both FortiGate devices.

   If both FortiGate devices are synchronized, the checksums match.

7. Alternatively, you can run the following CLI command on any member to view the checksums of all members:

   ```
   diagnose sys ha checksum cluster
   ```

Verify FortiGate Roles in an HA Cluster

After the checksums of both FortiGate devices match, you will verify the cluster member roles to confirm the primary and secondary devices.

To verify FortiGate roles in an HA cluster

1. On both the Local-FortiGate CLI and Remote-FortiGate CLI, enter the following command to verify that the HA cluster is established:

   ```
   get system status
   ```

2. On both FortiGate devices, view the Current HA mode line, and then write down the device serial number (Serial-Number).

   Notice that Local-FortiGate is a-p primary and Remote-FortiGate is a-p secondary.

3. On the Local-FortiGate CLI, enter the following command to confirm the reason for the primary election:

   ```
   get system ha status
   ```

4. In the output, look for the Primary selected using section to identify the reason for the latest primary election event.

   Your output should look like the following example:

   ```
   Primary selected using:
       <2023/09/21 10:52:56> vcluster-1: FGVM010000064692 is selected as the primary
    because its override priority is larger than peer member FGVM010000065036.
   ```