Contents

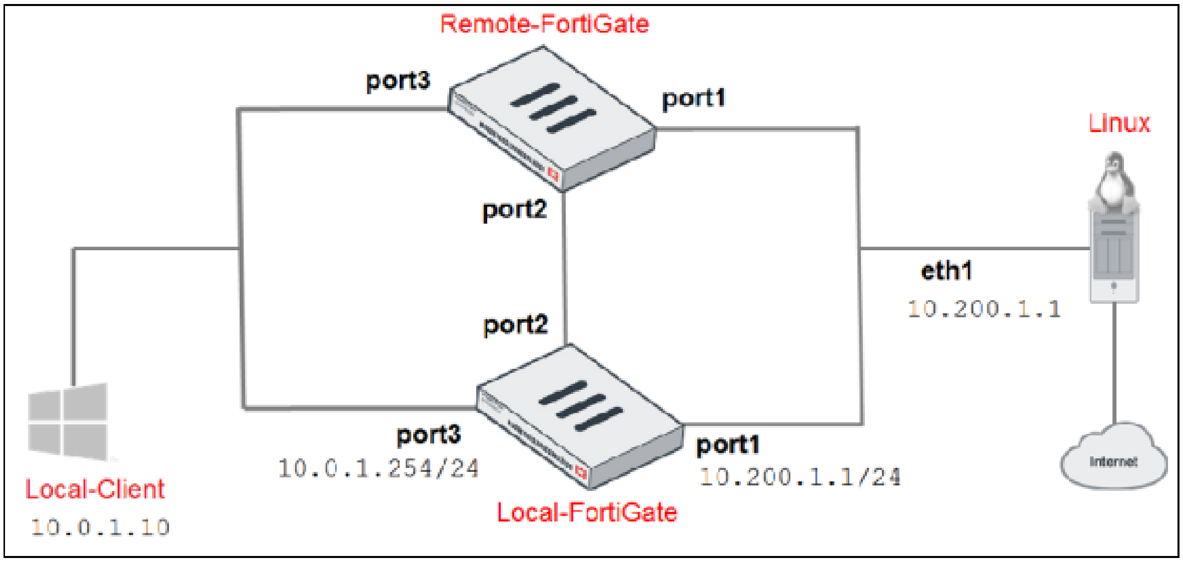
The objective

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-active 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 individually for management purposes:

1. Set up an HA cluster using FortiGate devices
2. l Observe HA synchronization and interpret diagnostic output
3. l Perform an HA failover
4. l Manage individual cluster members by configuring a reserved management interface

Topology

After you upload the required configurations to each FortiGate, the logical topology will change to the following:

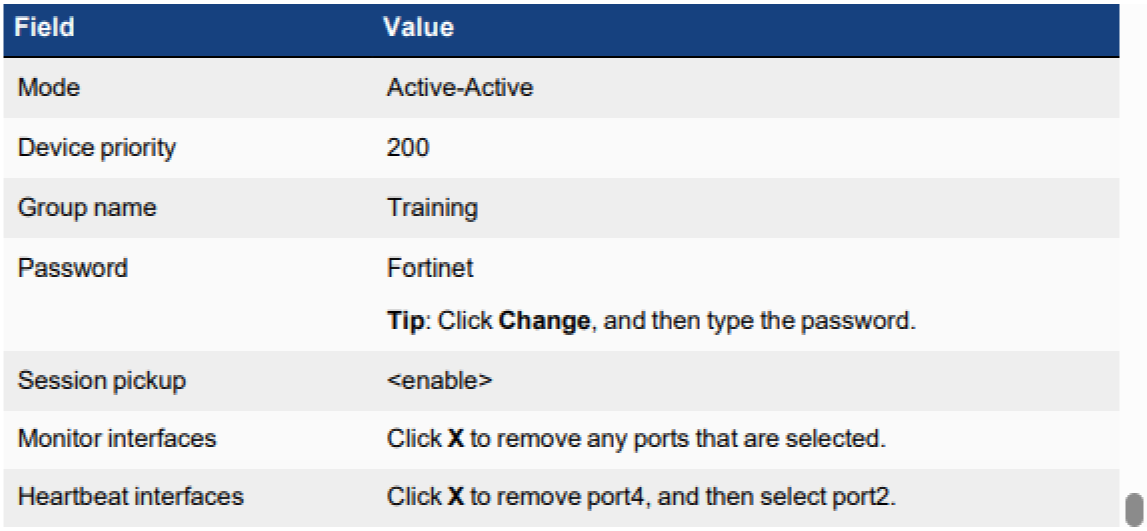


Components which used

1. Two FortiGate devices one act as a local and other as a Remote
2. Linux server
3. Local windows machine
4. Lab Environment like Fortinet Portal

Steps of this lab

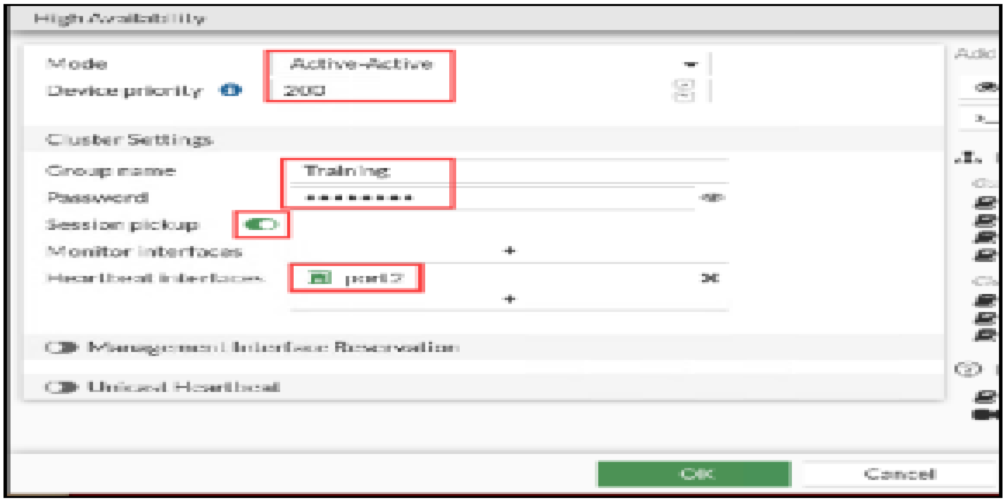
1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password.
2. 2. In the upper-right corner of the screen, click admin, and then click Configuration > Revisions.
3. Click + to expand the list.
4. Select the configuration with the comment local-ha, and then click Revert
5. Reboot
6. 1. Connect to the Remote-FortiGate GUI, and then log in with the username admin and password.
7. 2. In the upper-right corner of the screen, click admin, and then click Configuration > Revisions.
8. Click + to expand the list.
9. Select the configuration with the comment initial, and then click Revert.
10. Reboot
11. Connect to the Local-FortiGate GUI, and then log in with the username admin and password.
12. Click System > HA, and then configure the following HA settings



Field	Value
Mode	Active-Active
Device priority	200
Group name	Training
Password	Fortinet **Tip**: Click **Change**, and then type the password.
Session pickup	<enable>
Monitor interfaces	Click **X** to remove any ports that are selected.
Heartbeat interfaces	Click **X** to remove port4, and then select port2.

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

config system ha



High Availability

Mode: Active-Active

Device priority: 200

Cluster Settings

Group name: Training

Password: *********

Session pickup: ●

Monitor interfaces

Heartbeat interfaces: port2

```
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
```

Testing

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

- On the Remote-FortiGate CLI, you should see the debug messages about the HA synchronization process.
- These messages sometimes display useful status change information.
- 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.
- 4. To check the HA synchronization status, enter the following command:
- 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

The result

Test 1 & Result

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).

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

The output confirms that Local-FortiGate was elected primary because of its higher

priority.

If you see that the election reason is a higher uptime, then that is probably because

you rebooted one of the members, and as a result, the HA uptime of that device was

reset. The reboot then caused the HA uptime difference to be more than five

Test 2 & Result

1. On the Local-Client VM, open a browser, and then visit the following URL:
2. https://www.youtube.com
3. Play a long video (more than 5 minutes long).
4. While the video is playing, open a terminal, and then run a continuous ping to a public IP address:
5. ping 4.2.2.2
6. To trigger a failover, on the Local-FortiGate CLI, enter the following command to reboot Local-FortiGate:
7. execute reboot
8. Press Y to confirm that you want to reboot Local-FortiGate.
9. On the Local-Client VM, check the terminal and video that you started earlier. Because of the failover, Remote-FortiGate is now the primary processor of traffic. Your ping and video should still be running. 2. Press Ctrl+C to stop the ping. 3. To verify that Remote-FortiGate is acting as the primary device in the HA cluster, on the Remote-FortiGate CLI, enter the following command: get system status

   The output of get system ha status has been cut to fit this page. Local-FortiGate becomes the secondary device in the cluster because it has a lower HA uptime than Local-Remote. In addition, the HA uptime difference between the members is more than 5 minutes.