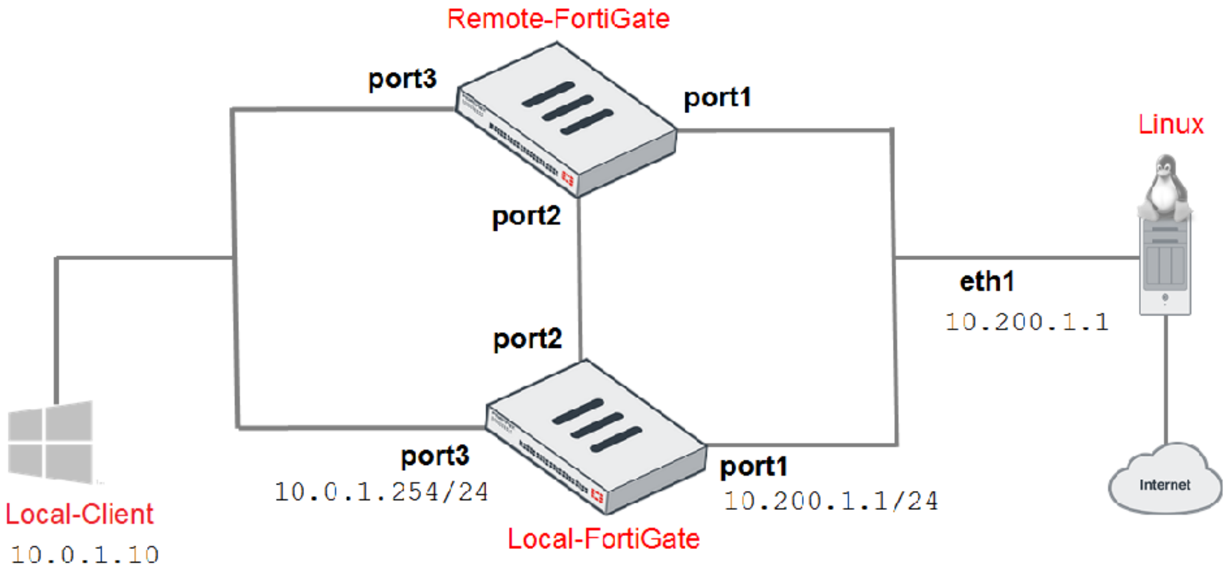
High Availability

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

Topology



Components used

1- Local-FortiGate
2- Remote-FortiGate
3- Local-Client

Steps of the lab

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.

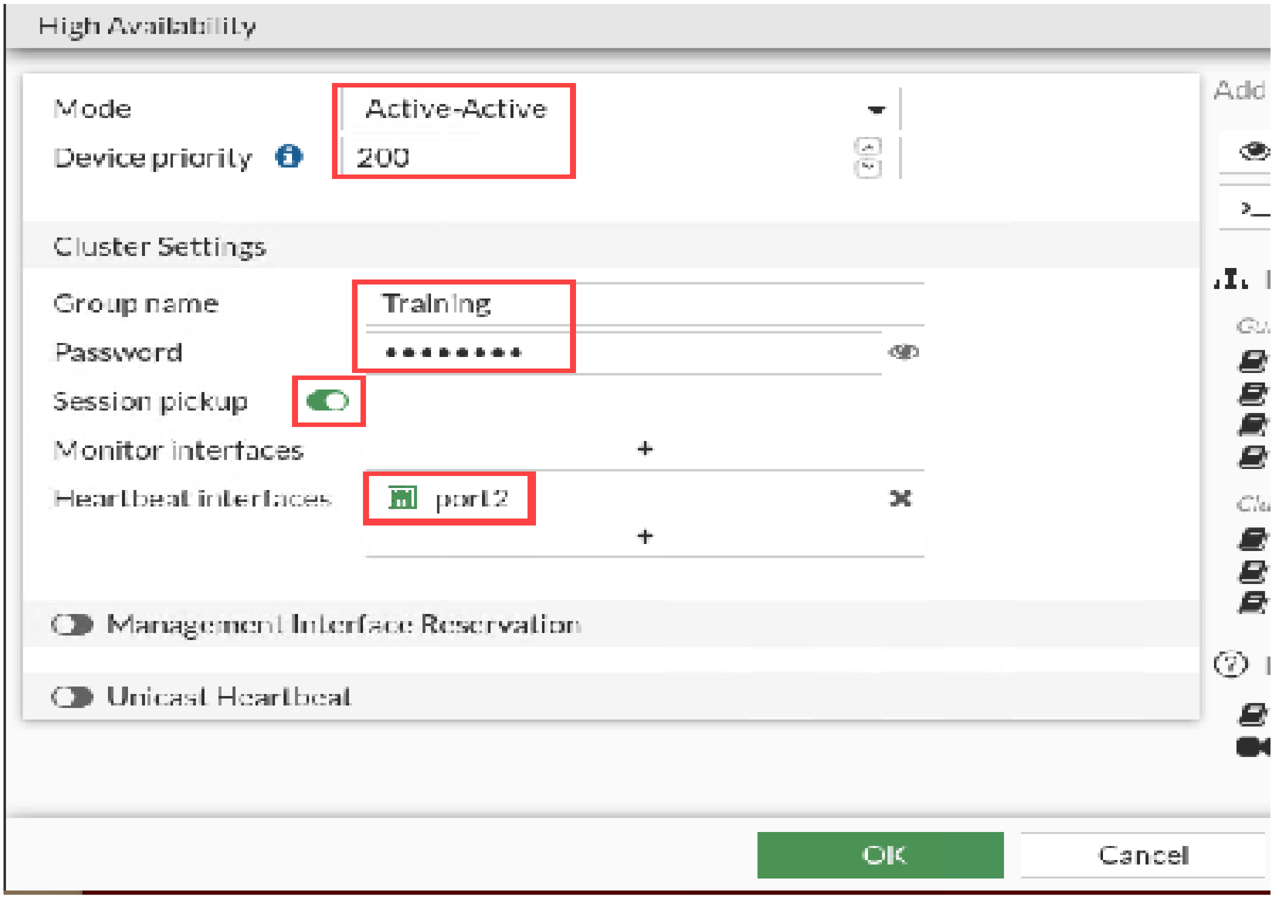
Configure HA Settings on Local-FortiGate

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 password.

2. Click System > HA, and then configure the following HA settings:



High Availability

Mode: Active-Active

Device priority: 200

Cluster Settings

Group name: Training

Password: •••••••••

Session pickup: on

Monitor interfaces

Heartbeat interfaces: port2

Management Interface Reservation

Unicast Heartbeat

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 password.

2. Enter 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
```

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, you should see 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.

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

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-a primary and Remote-FortiGate is a-a 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.

Verify Firewall Policy Configuration

By default, a FortiGate HA active-active cluster load balances only sessions that are subject to proxy inspection.

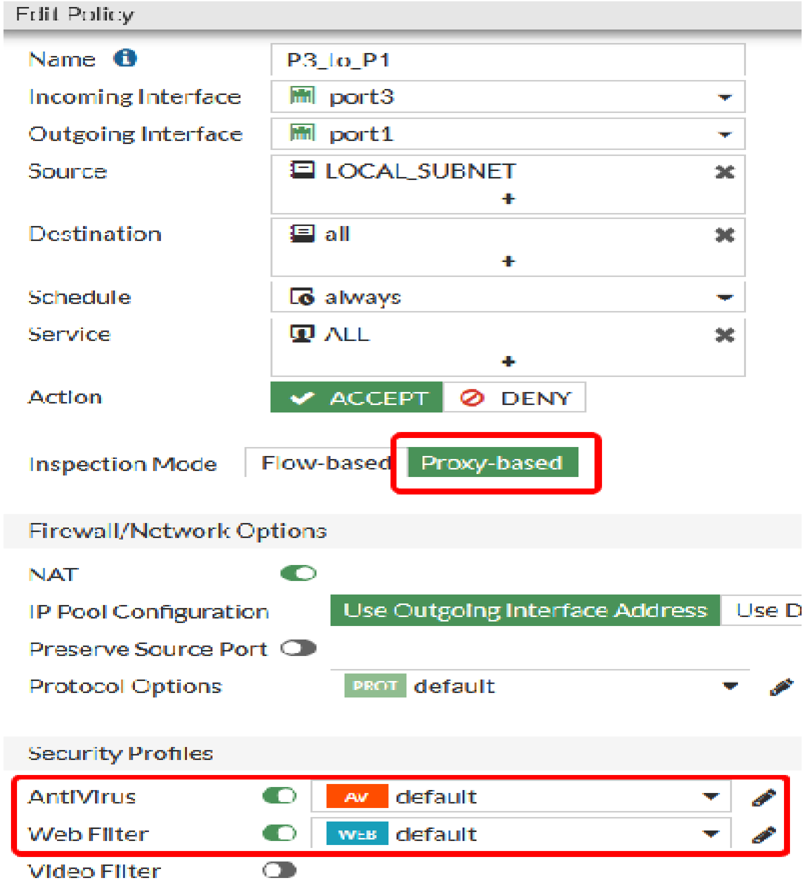
For this reason, you will verify that the matching firewall policy is configured to perform proxy inspection.

To verify firewall policy configuration

1. Continuing on the Local-FortiGate GUI, click Policy & Objects > Firewall Policy.

2. Double-click the firewall policy named P3_to_P1 to view its settings.

Your page should look similar to the following example:



Edit Policy

Name	P3_to_P1
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY
Inspection Mode	Flow-based [✓ Proxy-based]

Firewall/Network Options

NAT	●
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use D
Preserve Source Port	○
Protocol Options	PROT default

Security Profiles

AntiVirus ●	AV default
Web Filter ●	WEB default
Video Filter ○	

3. Click Cancel

View Session Statistics

You will view session statistics.

To view session statistics

1. On the Local-Client VM, open a few browser tabs, and connect to a few websites, such as:

l https://docs.fortinet.com

l www.yahoo.com

l www.bbc.com

2. On both the Local-FortiGate CLI and Remote-FortiGate CLI, enter the following command:

```
get system session status
```

Exercise 2: Triggering an HA Failover

You set up an HA cluster. In this exercise, you will examine how to trigger an HA failover, and observe the

renegotiation among devices to elect a new primary device and redistribute the sessions.

Trigger a Failover by Rebooting the Primary FortiGate

To trigger a failover by rebooting the primary FortiGate

1. On the Local-Client VM, open a browser, and then visit the following URL:

https://www.youtube.com

2. Play a long video (more than 5 minutes long).

3. While the video is playing, open a terminal, and then run a continuous ping to a public IP address:

```
ping 4.2.2.2
```

4. To trigger a failover, on the Local-FortiGate CLI, enter the following command to reboot Local-FortiGate:

```
execute reboot
```

5. Press Y to confirm that you want to reboot Local-FortiGate.

Verify the HA Failover and FortiGate Roles

You will verify the HA failover, and check the roles of FortiGate in an HA cluster.

To verify the HA failover and FortiGate roles

1. 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,

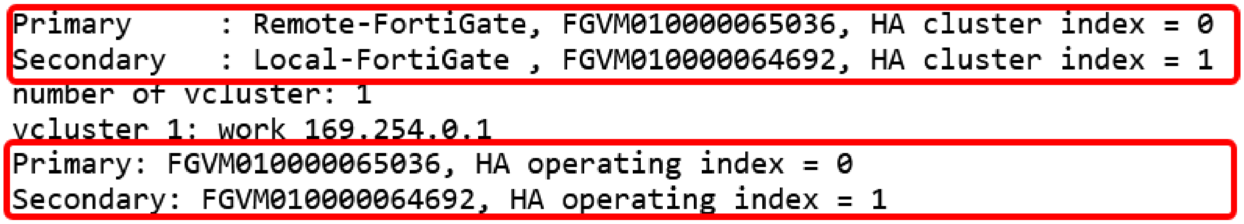
enter the following command:

get system status

4. To see the status of all cluster members, enter the following command on any FortiGate in the cluster:

get system ha status

You should see that Local-FortiGate rejoins the cluster as a secondary device. It lost its role as the primary device.



```
Primary     : Remote-FortiGate, FGVM010000065036, HA cluster index = 0
Secondary   : Local-FortiGate , FGVM010000064692, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Primary: FGVM010000065036, HA operating index = 0
Secondary: FGVM010000064692, HA operating index = 1
```

Trigger an HA Failover by Resetting the HA Uptime

You will trigger a failover by resetting the HA uptime on the current primary FortiGate—which should be Remote-

FortiGate—and then you will verify the role of Remote-FortiGate in the HA cluster.

To trigger an HA failover by resetting the HA uptime on FortiGate

1. On the Remote-FortiGate CLI console, enter the following command:

```
diagnose sys ha reset-uptime
```

2. On the Remote-FortiGate CLI, enter the following command to verify this:

```
get system status
```

Observe HA Leave and Join Messages Using Diagnostic Commands

The HA synchronization process is responsible for FGCP packets that communicate cluster status and build the

cluster. You will use real-time diagnostic commands to observe this process.

1. On the Local-FortiGate CLI, enter the following commands:

```
diagnose debug enable

diagnose debug application hatalk 0

diagnose debug application hatalk 255
```

2. On the Remote-FortiGate CLI, enter the following command to reboot Remote-FortiGate:

```
execute reboot
```

3. Press Y to confirm that you want to reboot Remote-FortiGate.

4. On the Local-FortiGate CLI, view the output while the secondary device reboots and starts communicating with the cluster.

5. To stop the debug output on Local-FortiGate, press the up arrow key twice, select the second-last command (in

this case, diagnose debug application hatalk 0), and then press Enter

Exercise 3: Configuring the HA Management Interface

In this exercise, you will examine how to configure a spare interface in the cluster as a reserved HA management

interface. This allows both FortiGate devices to be reachable for management purposes regardless of the

member role.

If a reserved HA management interface is not configured, your cluster management connections are handled by

the primary FortiGate. However, you can access the CLI of the secondary FortiGate from the primary FortiGate

CLI, or by using the secondary console connection.

You can also configure an in-band HA management interface, which is an alternative to the reserved HA

management interface, and does not require reserving an interface that is only for management access.

Access the Secondary FortiGate CLI Through the Primary FortiGate CLI

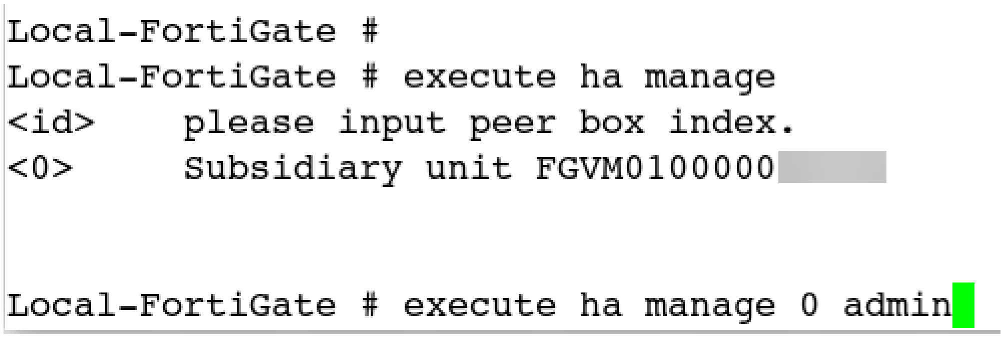
You will connect to the secondary FortiGate CLI through the primary FortiGate CLI.

To access the secondary FortiGate CLI through the primary FortiGate CLI

1. On the Local-FortiGate CLI, log in with the username admin and password password.

2. Enter the following command to access the secondary FortiGate CLI through the primary FortiGate heartbeat interface:

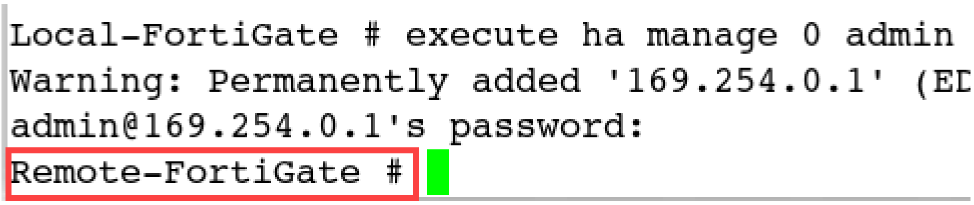
```
execute ha manage <id> admin
```



```
Local-FortiGate #
Local-FortiGate # execute ha manage
<id>    please input peer box index.
<0>     Subsidiary unit FGVM0100000[redacted]


Local-FortiGate # execute ha manage 0 admin
```

3. When prompted, enter the password password to log in to Remote-FortiGate.



```
Local-FortiGate # execute ha manage 0 admin
Warning: Permanently added '169.254.0.1' (ED
admin@169.254.0.1's password:
Remote-FortiGate #
```

4. Enter the following command to get the status of the secondary FortiGate:

get system status

5. View the Current HA mode line.

You will notice that Remote-FortiGate is a-a secondary.

6. Enter the following command to return to the Local-FortiGate CLI:

Exit

Set Up a Reserved HA Management Interface

You will use an unused interface on the FortiGate devices in an HA cluster to configure a reserved HA

management interface and a unique IP address on each member. This way, you can access each member

directly regardless of its role.

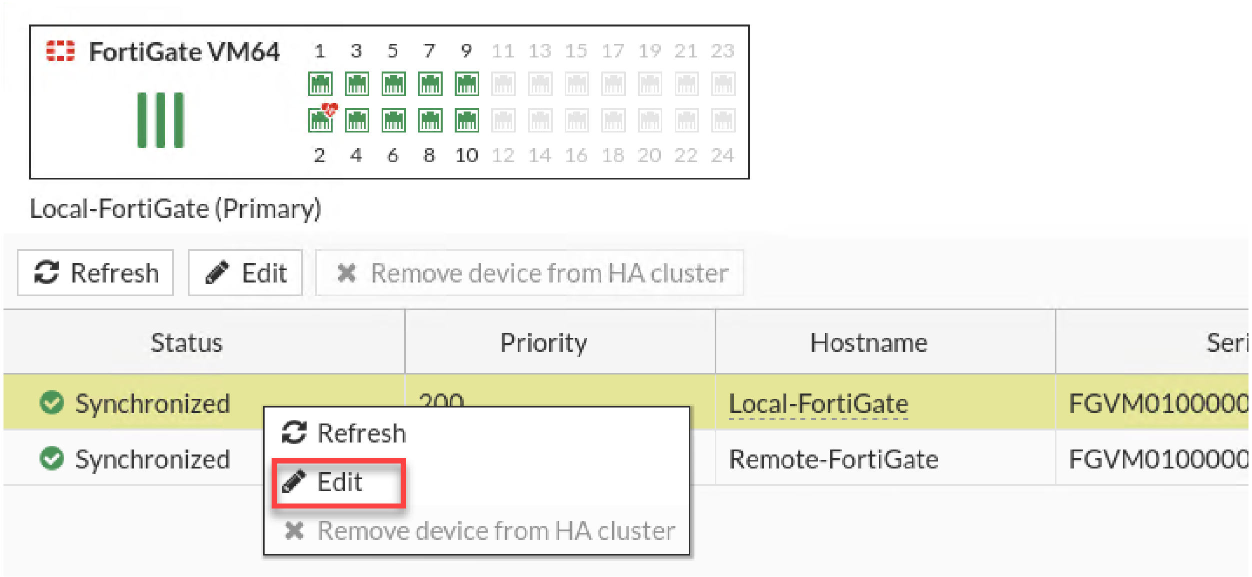
To set up a reserved HA management interface

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at 10.0.1.254 with the

username admin and password password.

2. Click System > HA.

3. Right-click Local-FortiGate, and then click Edit.



Status	Priority	Hostname	Seri
Synchronized	200	Local-FortiGate	FGVM0100000
Synchronized		Remote-FortiGate	FGVM0100000

4. Enable Management Interface Reservation, and then in the Interface field, select port7.

5. Click OK.

Configure and Access the Primary FortiGate Using the Reserved HA Management Interface

You will configure and verify access to the primary FortiGate using the reserved HA management interface.

To configure and verify access to the primary FortiGate using the reserved HA management interface

1. On the Local-FortiGate CLI, log in with the username admin and password password.

2. Enter the following commands to configure port7:

```
config system interface

edit port7

set ip 10.0.1.253/24

set allowaccess ping ssh snmp http

end
```

3. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at 10.0.1.253 (note the IP

address) with the username admin and password password.

This verifies connectivity to port7.

Configure and Access the Secondary FortiGate Using the Reserved HA Management Interface

You will configure and verify access to the secondary FortiGate using the reserved HA management interface.

To configure and verify access to the secondary FortiGate using the management interface

1. On the Remote-FortiGate CLI, enter the following command to verify that the reserved HA management interface

was synchronized with the secondary device:

```
show system ha
```

Look for ha-mgmt-status and config ha-mgmt-interfaces. These should already be set.

2. Enter the following command to verify that port7 has no configuration:

```
show system interface port7
```

3. Configure port7, using the following commands:

```
config system interface

edit port7

set ip 10.0.1.252/24

set allowaccess ping ssh snmp http

next

end
```

4. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI at 10.0.1.252 (note the IP

address) with the username admin and password password.

This will verify connectivity to port7.

Each device in the cluster now has its own management IP address for monitoring purposes.

The results

In this lab, you examined how to set up a FortiGate Clustering Protocol (FGCP) high availability (HA) cluster of FortiGate devices.

You explored active-active HA mode and observe FortiGate HA behavior.

You also performed an HA failover and used diagnostic commands to observe the election of a new primary device in the cluster.

Finally, you configured management ports on FortiGate devices to reach each FortiGate individually for management purposes.

Good Luck !