Name : Radwa Talaat Ahmed

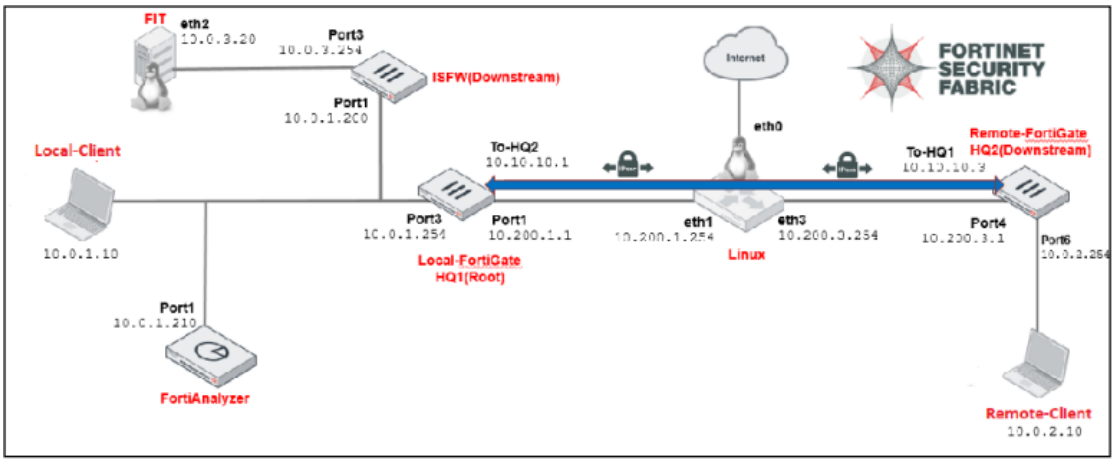
Security Fabric

The Objective :

In this lab, you will learn to configure the Fortinet Security Fabric. After you configure the Security Fabric, you will access the physical and logical topology views

- Configure the Security Fabric on Local-FortiGate (root) and ISFW (downstream)
- Configure the Security Fabric on Local-FortiGate (root) and Remote-FortiGate (downstream)
- Use the Security Fabric topology views to examine the logical and physical views of your network topology
- Run the Security Fabric rating checks on the root FortiGate and apply a recommendation

Topology :



Component Used :

- Two Fortigate Devices (Local Fortigate , Remote Fortigate)
- Local Windows Machine
- FortiAnalyzer
- Internal Segmentation Firewall
- Linux Server

Steps of This Lab :

➢ To restore the Remote-FortiGate configuration

1. Connect to the Remote-FortiGate GUI, and then log in with the username admin and password password.
2. In the upper-right corner of the screen, click admin, and then click Configuration > Revisions.
3. Click the + sign to expand the list.
4. Select the configuration with the comment remote-SF, and then click Revert
5. Click OK to reboot.

➢ To restore the Local-FortiGate configuration

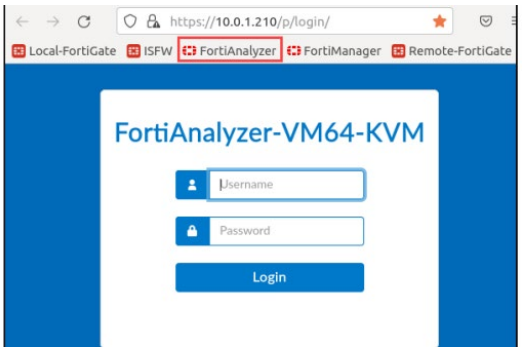
1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password password
2. In the upper-right corner of the screen, click admin, and then click Configuration > Revisions.
3. Click the + sign to expand the list
4. Select the configuration with the comment local-SF, and then click Rever
5. Click OK to reboot.

➢ To restore the ISFW configuration

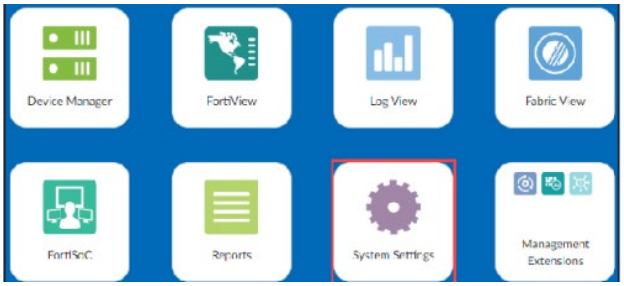
1. Connect to the ISFW GUI, and then log in with the username admin and password password.
2. In the upper-right corner of the screen, click admin, and then click Configuration > Revisions.
3. Click the + sign to expand the list
4. Select the configuration with the comment ISFW-SF, and then click Revert.
5. Click OK to reboot.

➢ To restore the FortiAnalyzer configuration

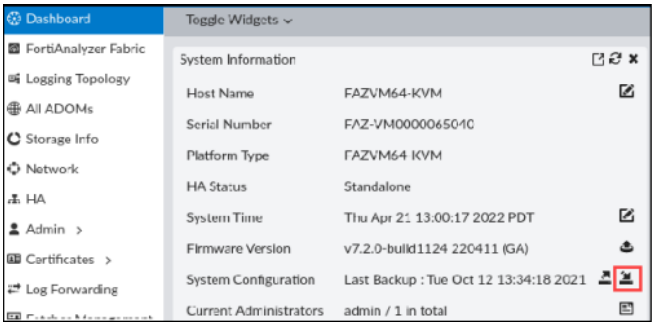
1. On the Local-Client VM, open a browser, and then connect to the FortiAnalyzer GUI at http://10.0.1.210
2. Log in to the FortiAnalyzer GUI with the username admin and password password. A link to FortiAnalyzer is added to the favorites bar in the browser on the Local-Client VM



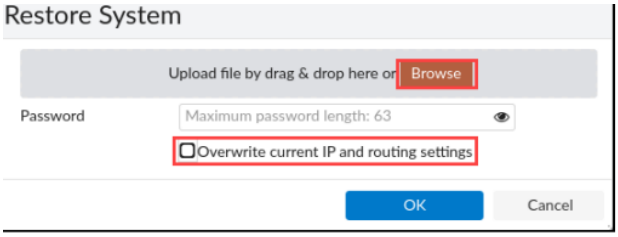
3. Click System Settings.



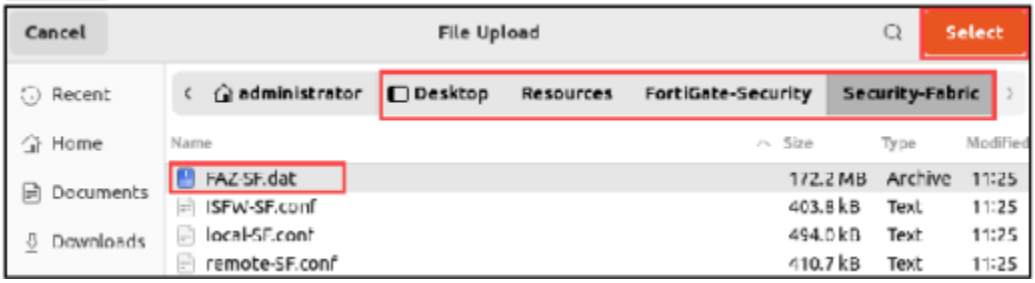
4. In the System Information section, click the icon to restore from an existing configuration



5. Clear the Overwrite current IP and routing settings checkbox, and then click Browse



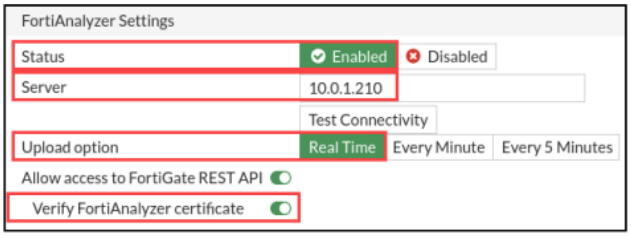
6. Browse to Desktop > Resources > FortiGate-Security > Security-Fabric, select FAZ-SF.dat, and then click Select.



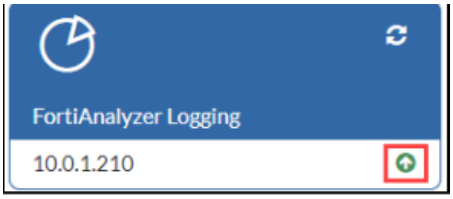
7. Click OK.
8. Wait until FortiAnalyzer restarts

➢ To configure Local-FortiGate to send logs to FortiAnalyzer

1. Log in to the Local-FortiGate GUI with the username admin and password password.
2. In the menu on the left, click Security Fabric > Fabric Connectors.
3. Select FortiAnalyzer Logging, and then click Edit.
4. Enable FortiAnalyzer Logging.
5. Edit the settings so they match the following image

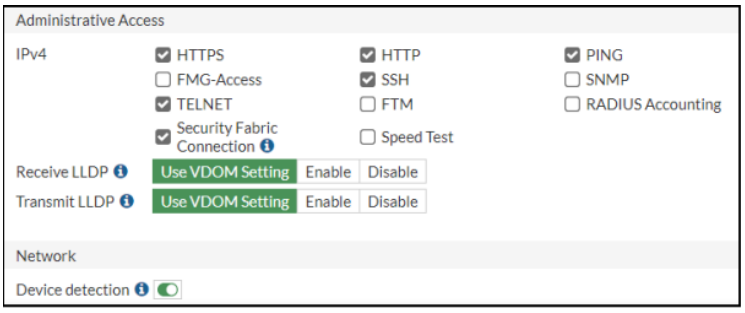


6. Click OK.
7. In the verification window that appears, click Accept
8. Verify that the status of Security Fabric > Fabric Connectors > FortiAnalyzer Logging is up



➢ To enable the Security Fabric connection on Local-FortiGate interfaces

1. On the Local-FortiGate GUI, log in with the username admin and password password
2. Click Network > Interfaces
3. Click port3, and then click Edit
4. In the Administrative Access section, select the Security Fabric Connection checkbox.
5. In the Network section, enable Device detection.



6. Click OK.
7. Click Network > Interfaces, and then expand port1
8. Click the To-Remote-HQ2 interface, and then click Edit.
9. In the Administrative Access section, select the Security Fabric Connection checkbox
10. Click OK.

➢ To enable the Security Fabric on Local-FortiGate

1. On the Local-FortiGate GUI, click Security Fabric > Fabric Connectors.
2. Click Security Fabric Setup, and then click Edit.
3. In the Security Fabric Settings section, click Enabled.
4. Click Serve as Fabric Root.
5. Configure the following settings:

Field	Value
Fabric name	fortinet
Allow other Security Fabric devices to join	enable
(ensure both interfaces are selected)	port3, To-Remote-HQ2

Your configuration should look like the following example:

6. Click OK.

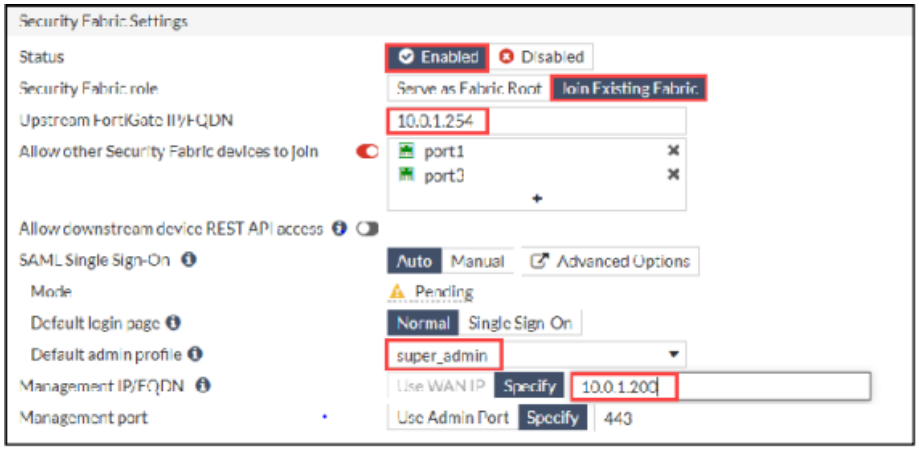
➢ To enable the Security Fabric connection on ISFW interfaces

1. On the ISFW GUI, log in with the username admin and password password.
2. Click Network > Interfaces
3. Click port1, and then click Edit
4. In the Administrative Access section, confirm that the Security Fabric Connection checkbox is selected.
5. In the Network section, enable Device detection.
6. Click OK.
7. Click Network > Interfaces
8. Click port3, and then click Edit.
9. In the Administrative Access section, select the Security Fabric Connection checkbox
10. In the Network section, enable Device detection.
11. Click OK to save the changes.

➢ To enable the Security Fabric on ISFW (downstream)

1. On the ISFW GUI, click Security Fabric > Fabric Connectors
2. Click Security Fabric Setup, and then click Edit
3. In the Security Fabric Settings section, click Enabled.
4. In the Security Fabric role field, confirm that Join Existing Fabric is selected
5. Verify that the Upstream FortiGate IP is set to 10.0.1.254
6. In the Default admin profile field, select super_admin

7. In the Management IP/FQDN field, click Specify, and then type 10.0.1.200.
   Your configuration should look like the following example

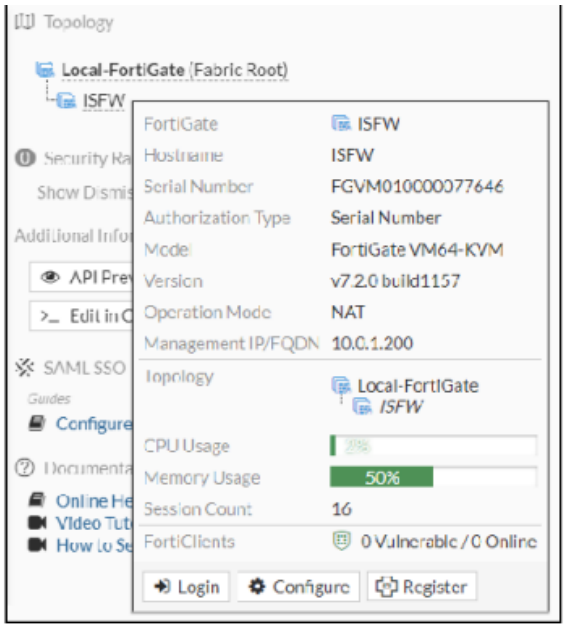


8. Click OK.
9. Click OK to confirm the settings

➢ To authorize ISFW on Local-FortiGate

1. On the Local-FortiGate GUI, click Security Fabric > Fabric Connectors
2. In the Topology section, click the highlighted FortiGate serial number, and then click Authorize

3. In the Device Registration window, click Authorize, and then click Close.
4. Hover over the ISFW icon to display a summary of the firewall settings, and then verify that it is correctly registered in the Security Fabric.

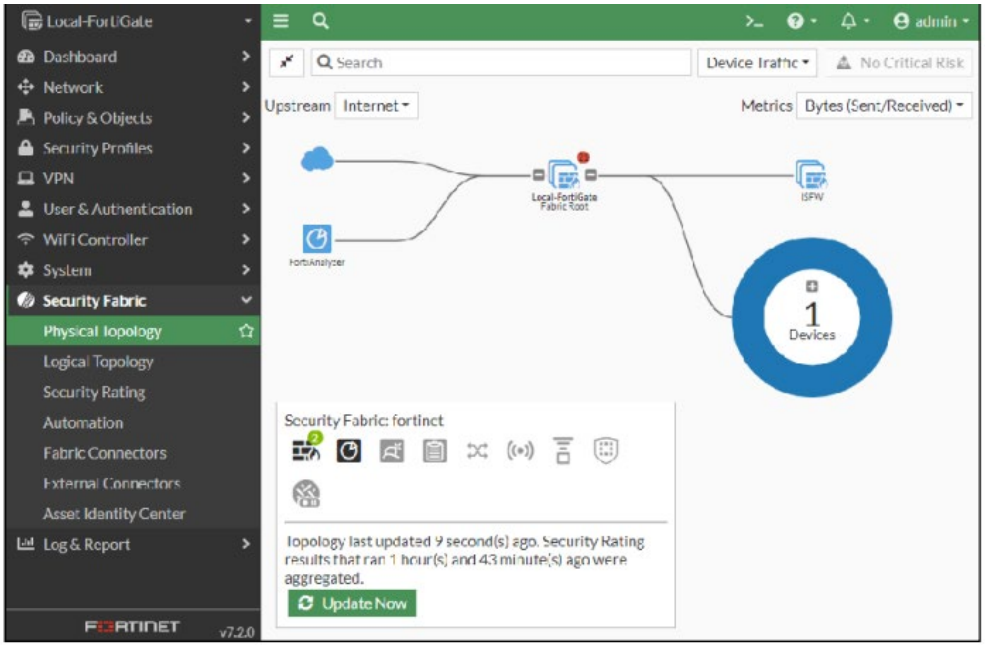


➢ The Testing

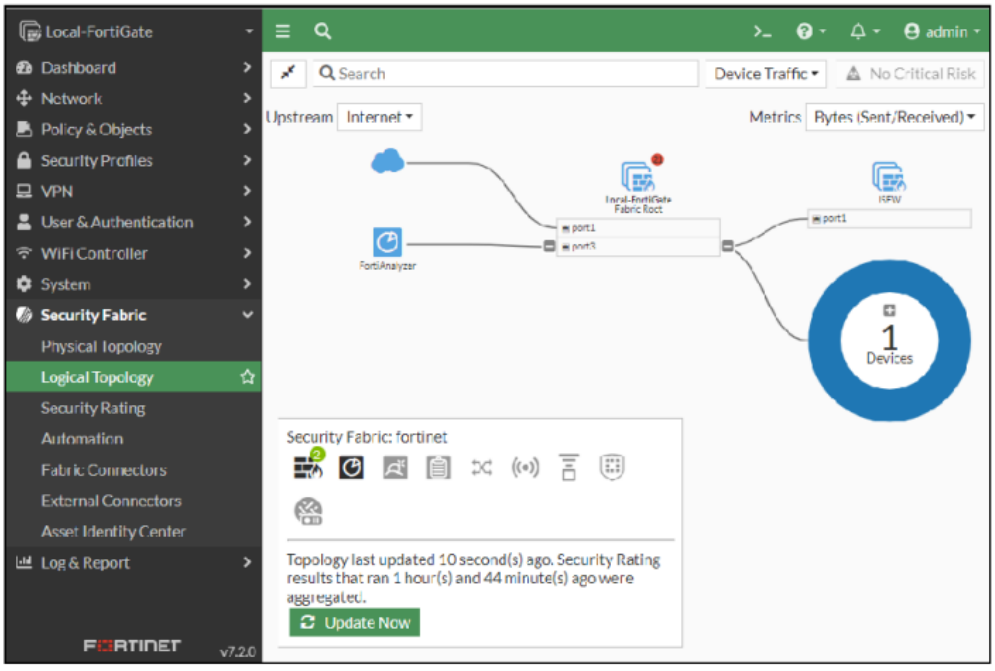
Test the security fabric Deployment

To check the Security Fabric on Local-FortiGate

1. On the Local-Client VM, open a new browser, and then go to https://www.fortinet.com. This is to generate some traffic from the Local-Client VM so it is included in the topology views
2. On the Local-FortiGate GUI, click Dashboard > Status. The Security Fabric widget displays the FortiGate devices in the Security Fabric.
3. On the Local-FortiGate GUI, click Security Fabric > Physical Topology. This page shows a visualization of access layer devices in the Security Fabric.



4. On the Local-FortiGate GUI, click Security Fabric > Logical Topology. This dashboard displays information about the interfaces that connect each device in the Security Fabric



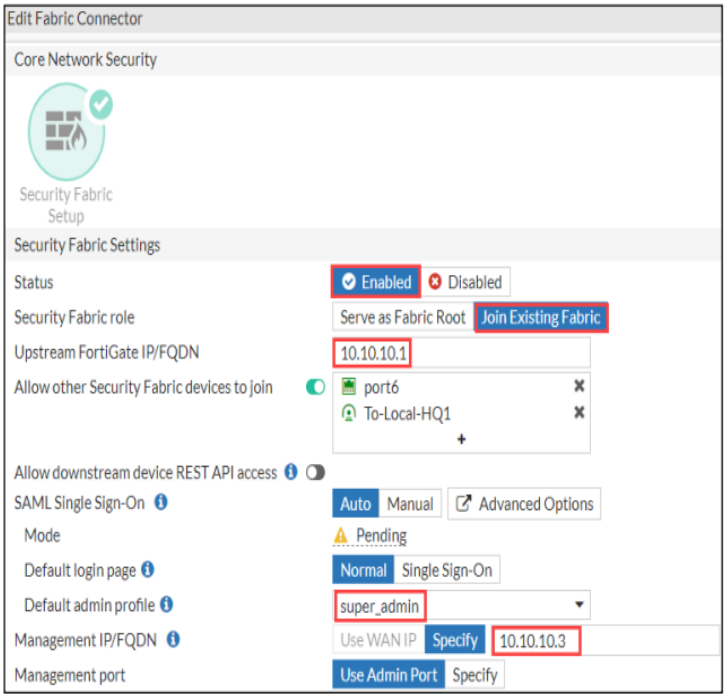
- To enable the Security Fabric connection on Remote-FortiGate interfaces

1. On the Remote-FortiGate GUI, log in with the username admin and password password.
2. Click Network > Interfaces
3. Click port6, and then click Edit.
4. In the Administrative Access section, select the Security Fabric Connection checkbox
5. In the Network section, ensure that Device detection is enabled
6. Click OK.
7. Click Network > Interfaces, and then expand port4.
8. . Click the To-Local-HQ1 interface, and then click Edit.
9. In the Administrative Access section, select the Security Fabric Connection checkbox.
10. Click OK to save the changes.

- To enable the Security Fabric on Remote-FortiGate

1. . On the Remote-FortiGate GUI, click Security Fabric > Fabric Connectors.
2. Click Security Fabric Setup, and then click Edit.
3. In the Security Fabric Settings section, click Enabled.
4. In the Security Fabric role field, ensure that Join Existing Fabric is selected
5. In the Upstream FortiGate IP field, type 10.10.10.1.
6. In the Default admin profile field, select super_admin.
7. In the Management IP/FQDN field, click Specify, and then type 10.10.10.3

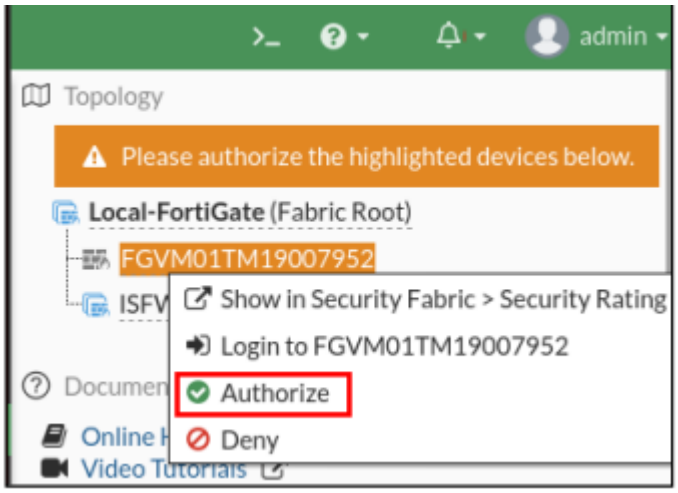
   Your configuration should look like the following example



8. Click ok
9. Click ok to confirm

➢ To authorize Remote-FortiGate on Local-FortiGate

1. On the Local-FortiGate GUI, log in with the username admin and password password
2. Click Security Fabric > Fabric Connectors
3. In the Topology section, click the highlighted FortiGate serial number, and then click Authorize.

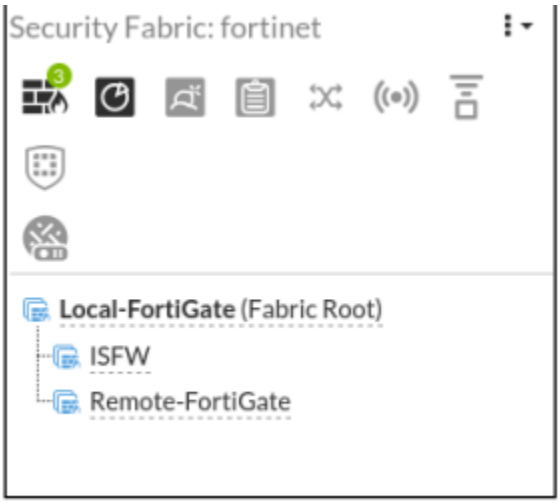


4. In the Device Registration window, click Authorize, and then click Close.

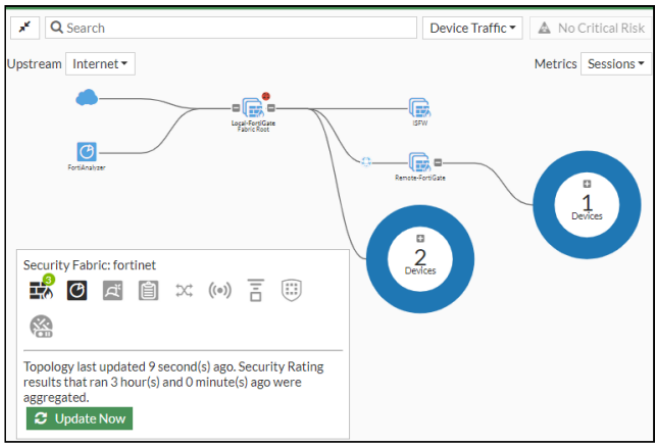
Testing :

➢ check the Security Fabric on Local-FortiGate

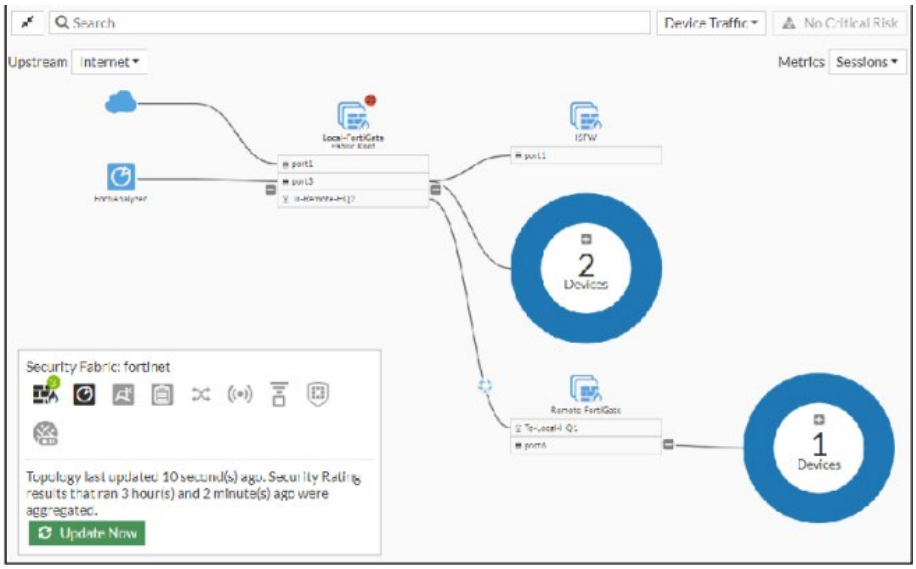
1. On the Local-FortiGate GUI, click Dashboard > Status. The Security Fabric widget displays all FortiGate devices in the Security Fabric.



2. Click Security Fabric > Physical Topology. This page shows a visualization of access layer devices in the Security Fabric.



3. Click Security Fabric > Logical Topology. This dashboard displays information about the interfaces that each device in the Security Fabric connects to.

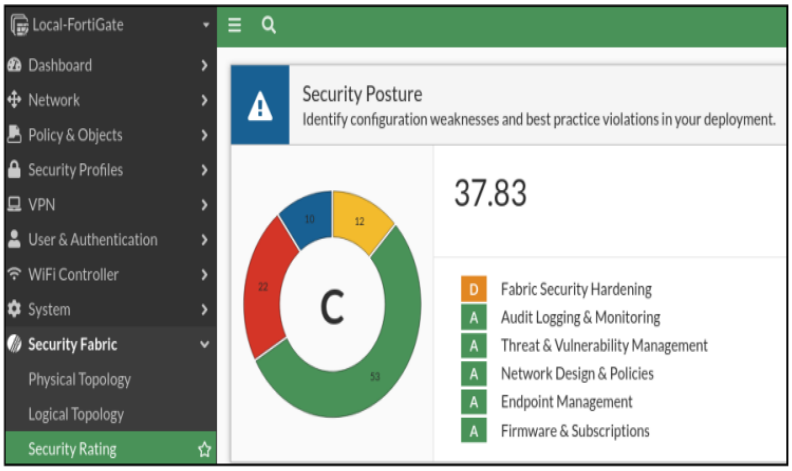

Search
Device Traffic
No Critical Risk
Upstream
Internet
Metrics
Sessions
port1
port3
2
Devices
Security Fabric: fortinet
Topology last updated 10 second(s) ago. Security Rating results that ran 3 hour(s) and 2 minute(s) ago were aggregated.
Update Now
1
Devices

The Results :

You will run a security rating check, which analyzes the Security Fabric deployment, and then identifies potential vulnerabilities and highlights best practices. You must run the Security Fabric rating on the root FortiGate in the Security Fabric.

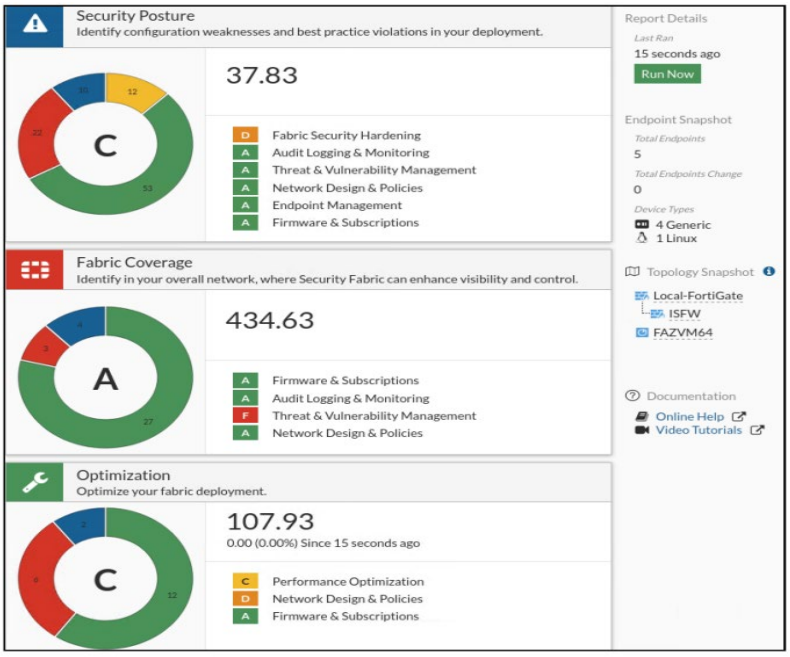
➢ To review the Security Posture widget

1. On the Local-FortiGate GUI, log in with the username admin and password password.
2. Click Security Fabric > Security Rating, and then check the Security Posture widget to see the score of your Security Fabric deployment



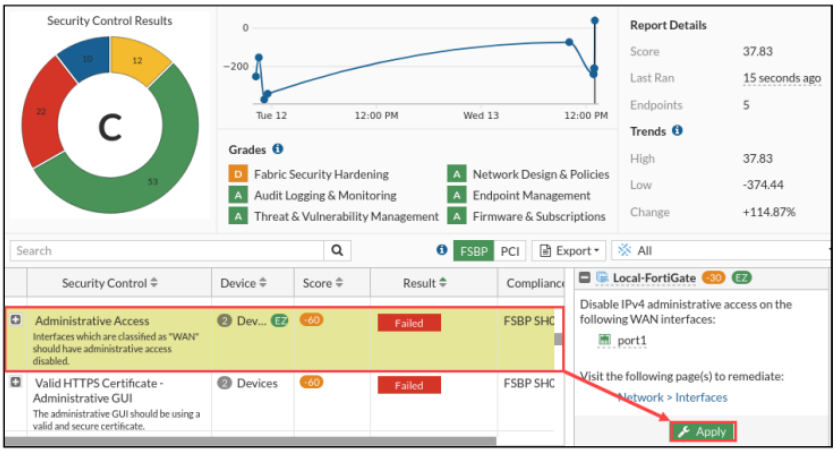
➢ To Generate new security rating scores on the root FortiGate

1. On the Local-FortiGate GUI, click Security Fabric > Security Rating



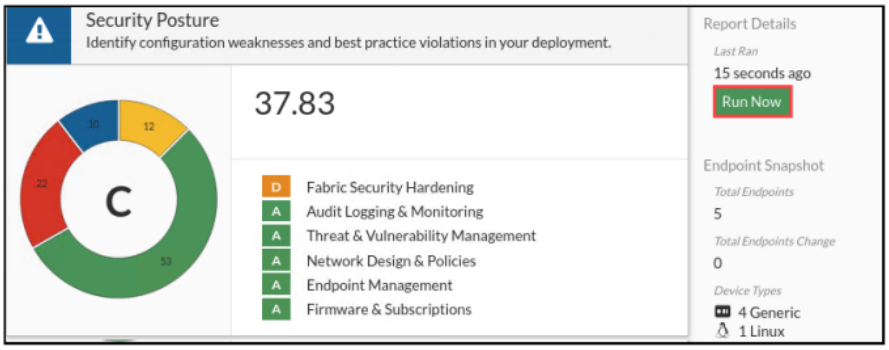
2. Click Security Posture to show the scorecard details

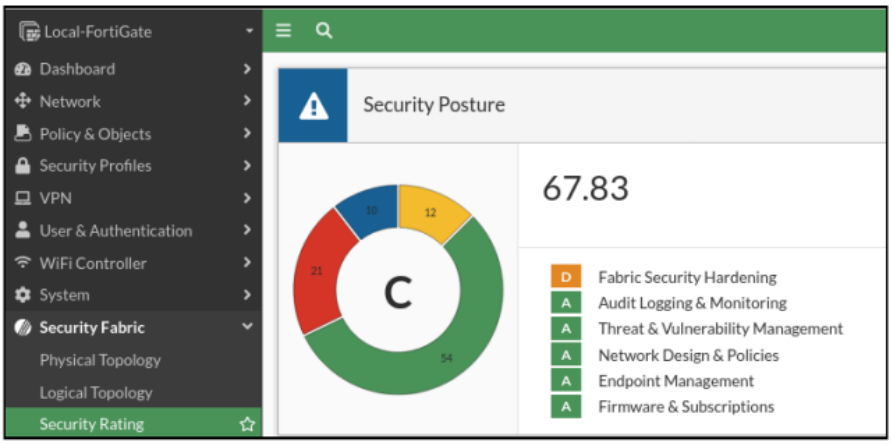
3. In the Security Control column, expand Failed, and then select Administrative Access. The Apply option appears with recommendations that the wizard can apply.
4. In the right pane, under Local-FortiGate, click Apply.



5. Click OK to save the configuration file. The View Diff button appears beside Apply after audit log settings are applied successfully.
6. Click View Diff to view the configuration changes that the wizard applied to Local-FortiGate.

7. Click Close
8. Click Security Fabric > Security Rating
9. Click Run Now to get the new Security Posture score


Security Posture
Identify configuration weaknesses and best practice violations in your deployment.
37.83
C
10
12
22
53
D Fabric Security Hardening
A Audit Logging & Monitoring
A Threat & Vulnerability Management
A Network Design & Policies
A Endpoint Management
A Firmware & Subscriptions
Report Details
Last Ran
15 seconds ago
Run Now
Endpoint Snapshot
Total Endpoints
5
Total Endpoints Change
0
Device Types
4 Generic
1 Linux


Local-FortiGate
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Physical Topology
Logical Topology
Security Rating
Security Posture
67.83
C
10
12
21
54
D Fabric Security Hardening
A Audit Logging & Monitoring
A Threat & Vulnerability Management
A Network Design & Policies
A Endpoint Management
A Firmware & Subscriptions