MIAARI ACADEMY
EDUCATION & IT SOLUTIONS

NSE5 FortiManager and FortiAnalyzer

VPN Hub & Spoke LAB Creating Community & Gateway Lab Part1# 80

Prepared by
Eng. Mahmoud Maari

➢ Accessing the FortiManager using the GUI with “miaari”:

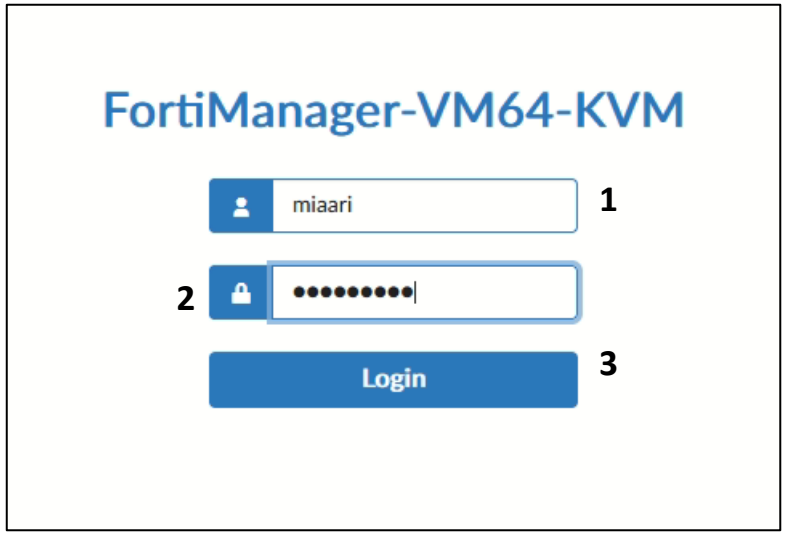
Open your browser and use the Management IP Address for the FMG in Data Center inside Head Quarter (10.10.10.200)

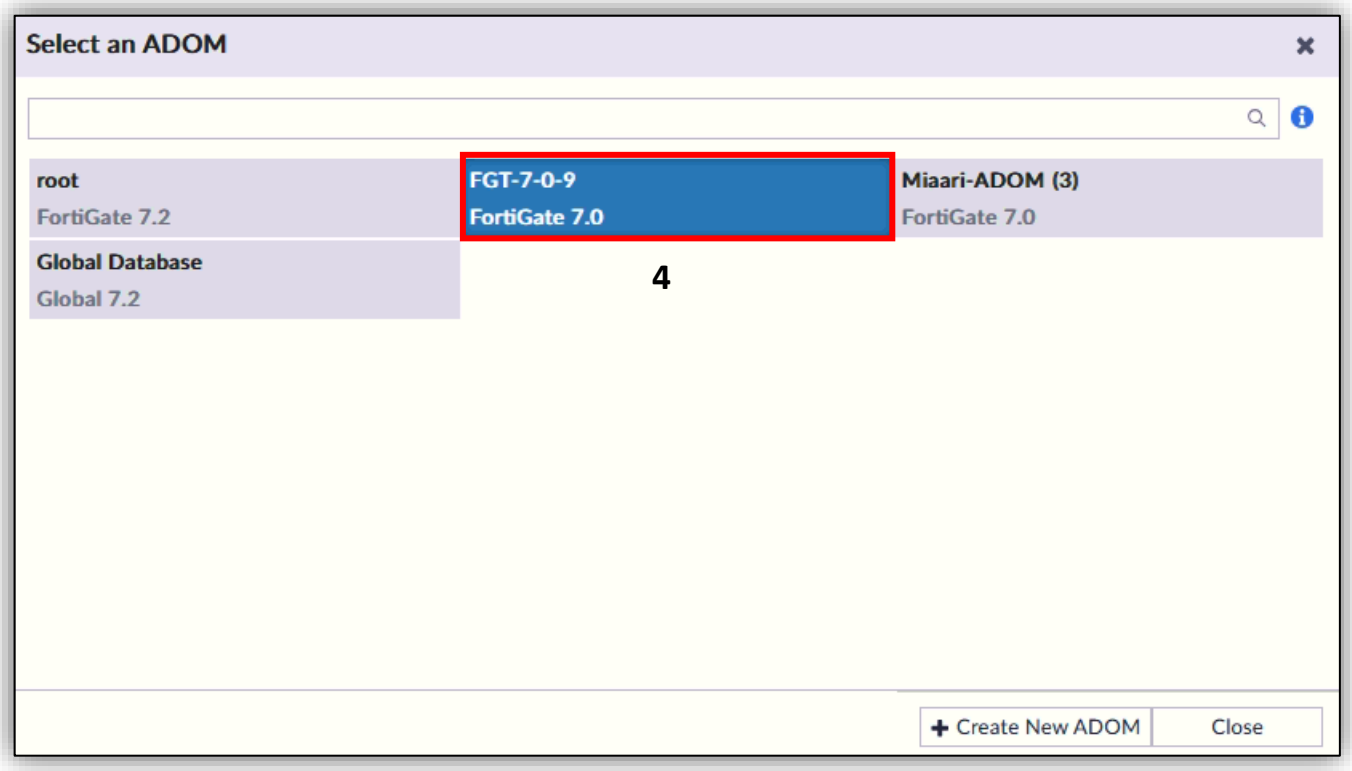
1.Enter Username (miaari)

2.Enter Password (admin@123)

3.Login

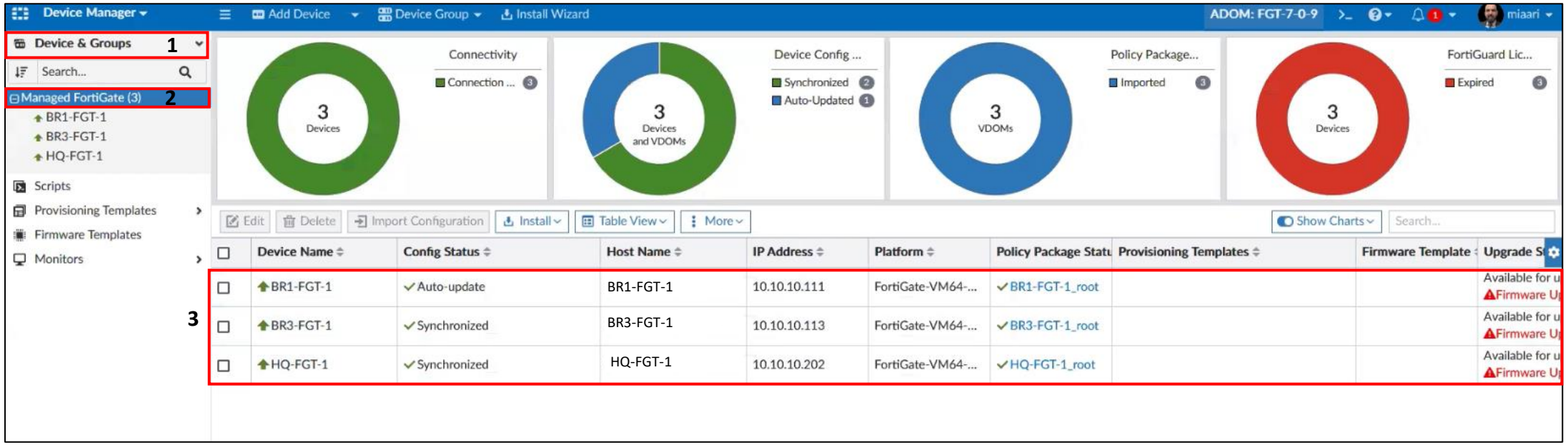
4.Select ADOM (FGT-7-0-9)





- To view devices in ADOM (FGT-7-0-9):

Click on “Device Manager”.



1. Click on "Device & Groups" section.
2. Select "Managed FortiGate," which, in this case, shows a total of 3 devices. This section lists all the FortiGate devices currently managed by the FortiManager.
3. There are details of the managed devices, including columns for Device Name, Config Status, Host Name, IP Address, Platform, Policy Package Status, and Provisioning Templates.

Config Status:

Auto-update: This ensures that any changes or updates made within the FortiManager are automatically pushed to the device without manual intervention.

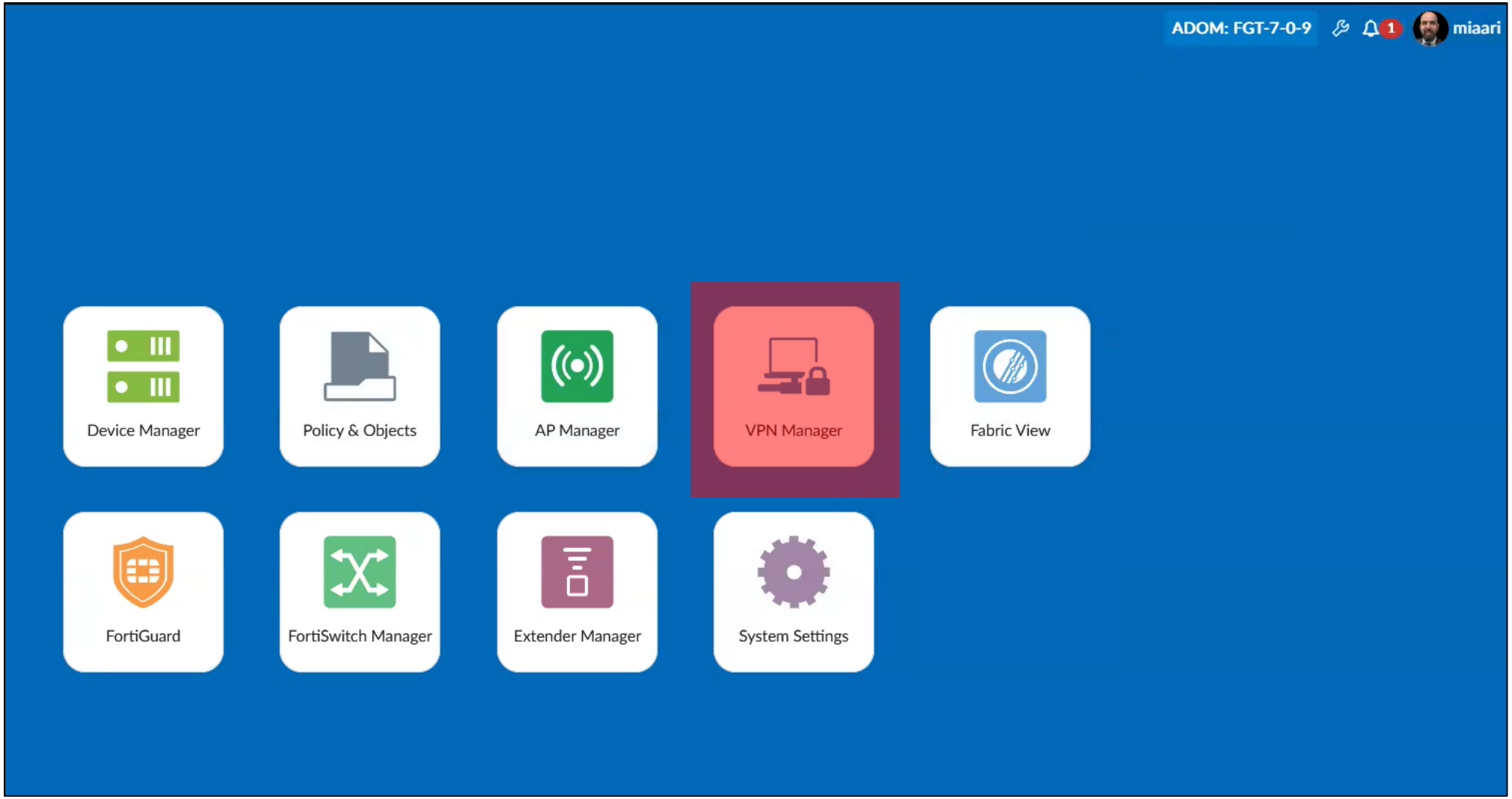
Synchronized: This status means that the configuration on FortiManager and the device is synchronized.

Policy Package Status:

The Policy Package Status column shows the status of the policy packages that are assigned to each device. In the image:

- To Create VPN between Branch-1 ,Branch-3 and Head Quarter.

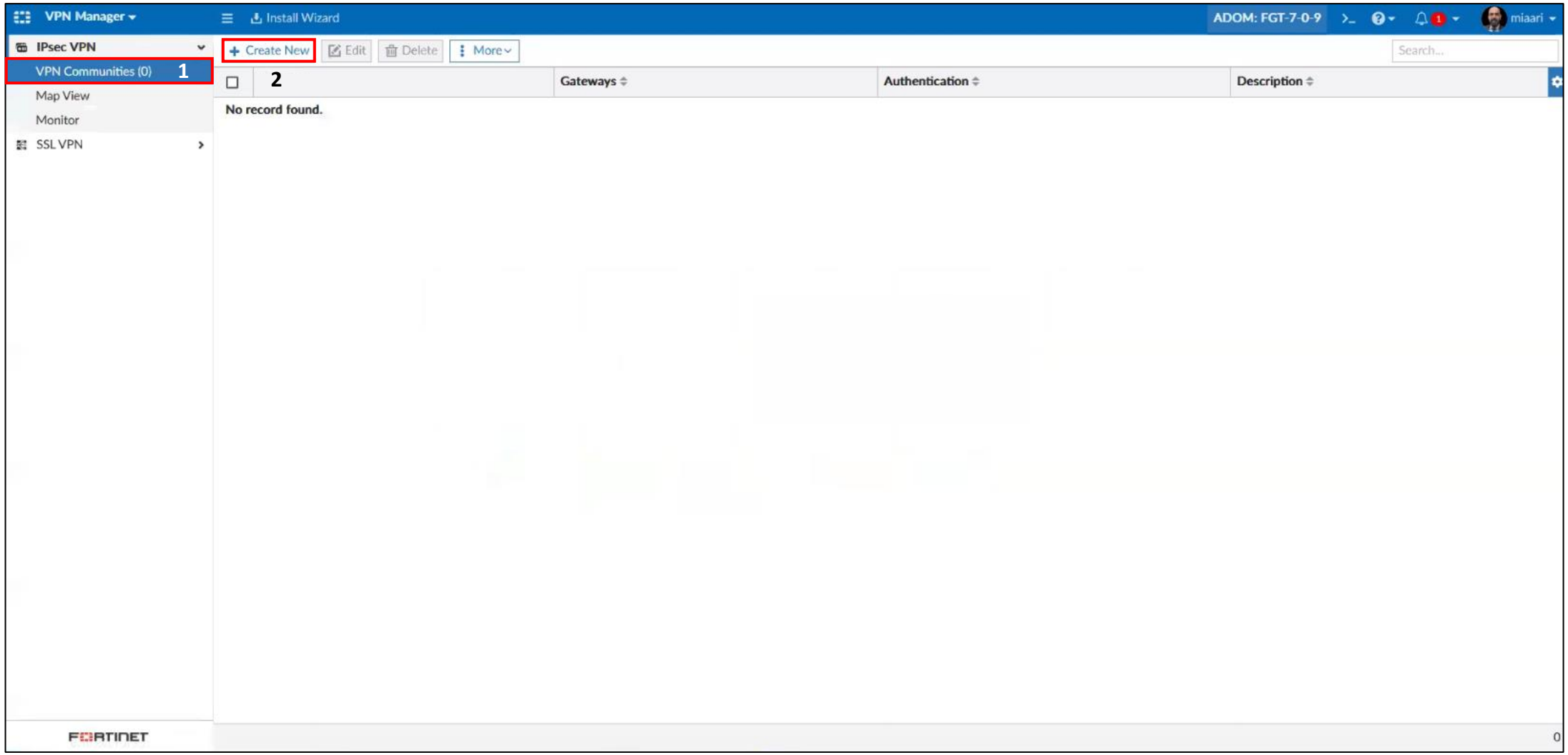
Click on “VPN Manager”.



- To create VPN community

1. Click on "VPN Communities" to manage and configure VPN communities.

2. Click on the "+ Create New" button located at the top right corner. This button allows you to start the process of creating a new IPsec VPN Community.



3. In the "Name" field, enter a descriptive name for your VPN Community "IPsec". This name should be unique and clearly identify the purpose or location of the VPN.

4. Choose the appropriate VPN topology for your community. The options provided are:

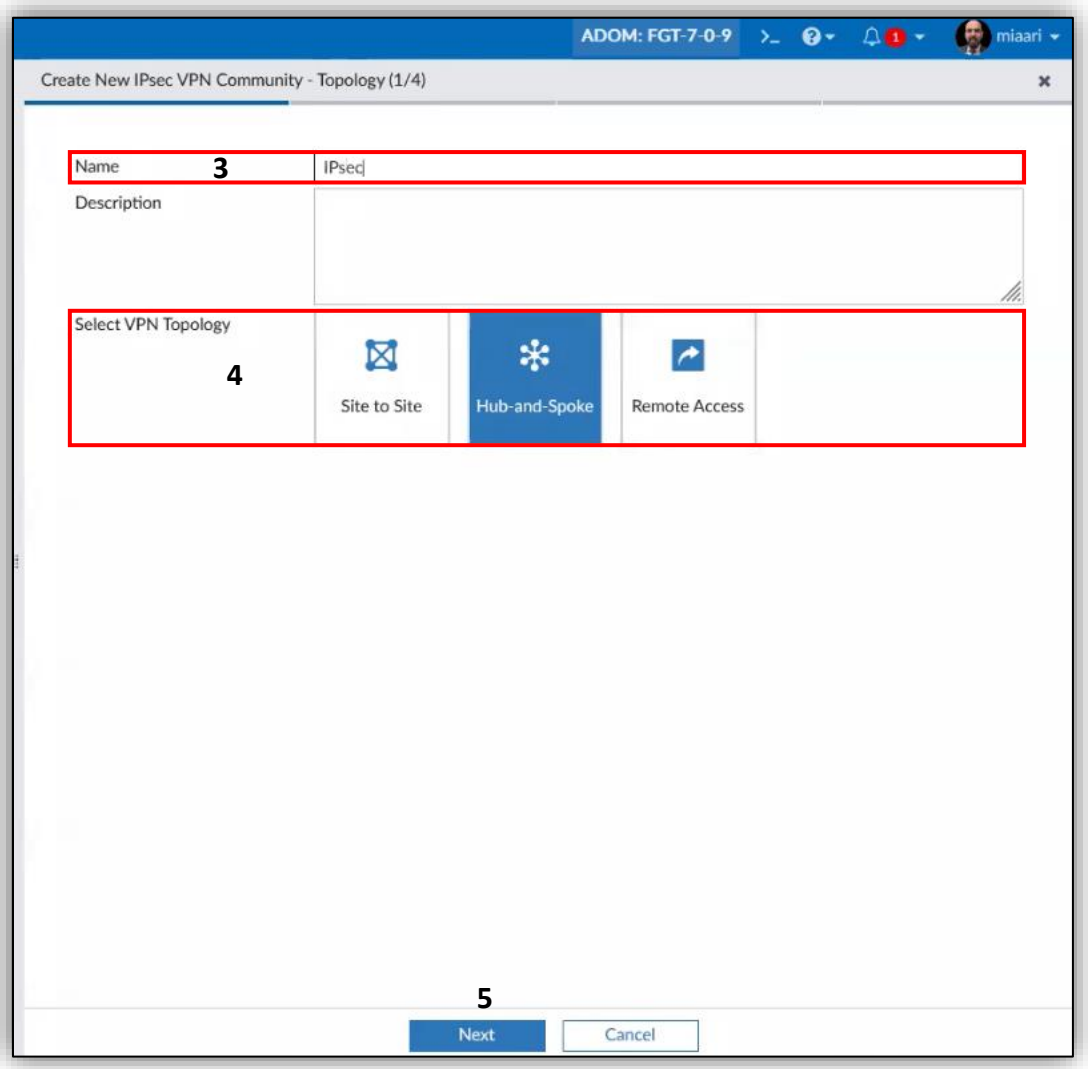
   Site to Site: Used for connecting two different locations, typically between different branch offices or between a branch office and headquarters.

   Hub-and-Spoke: Used when you have a central hub (e.g., headquarters) that connects to multiple spoke sites (e.g., branch offices).

   Remote Access: Used for allowing remote users to connect to the network securely from different locations.

   The "Hub-and-Spoke" topology is selected, indicating that this VPN community will connect multiple branch offices to a central hub.

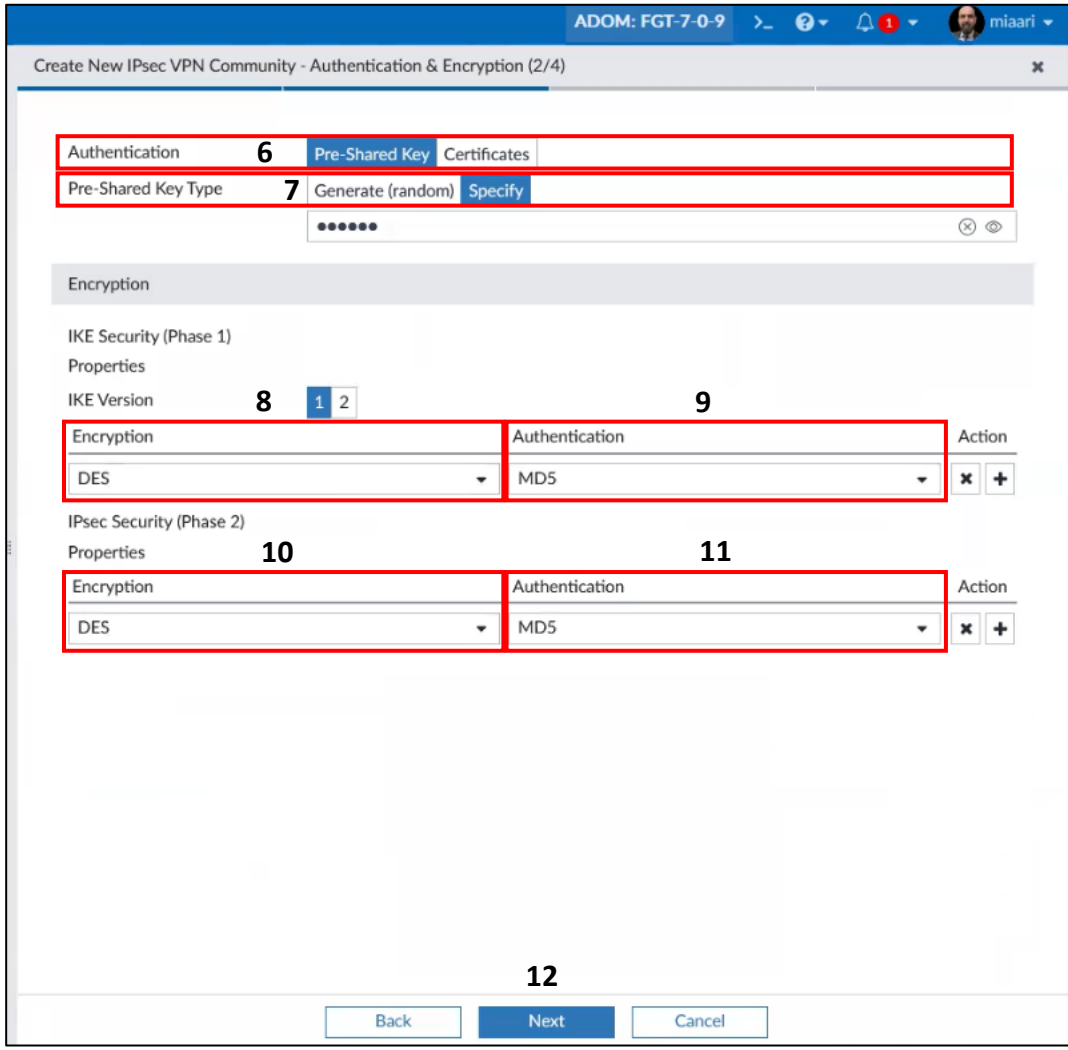
5. Once you've filled out the necessary details and selected the VPN topology, click on the "Next" button at the bottom right to proceed to the next step in the VPN community configuration.



6. Choose the type of authentication for the VPN connection. The available options are:

Pre-Shared Key: A secret key shared between both VPN endpoints. This is a common and straightforward method.

Certificates: Use digital certificates for authentication, which offers stronger security but requires a certificate infrastructure.



"Pre-Shared Key" is selected, indicating that this method will be used for authenticating the VPN connection.

7. If "Pre-Shared Key" is selected as the authentication method, you can either:

Generate (random): Allow the system to generate a random pre-shared key.

Specify: Manually enter a pre-shared key of your choice.

"Specify" is chosen, allowing the user to manually enter a pre-shared key (123456).

8. Select the encryption algorithm for the IKE (Internet Key Exchange) Phase 1. This phase is responsible for establishing the secure channel. The available options may include various encryption algorithms such as DES, 3DES, AES, etc.

"DES" is selected for encryption.

9. Choose the authentication algorithm for IKE Phase 1. This step ensures the integrity and authenticity of the communication.

"MD5" is selected as the authentication method.

Continue:

10. Select the encryption algorithm for IPsec Security (Phase 2). Phase 2 is responsible for securing the actual data packets.Similar to Phase 1, various encryption algorithms are available.

"DES" is selected for encryption.

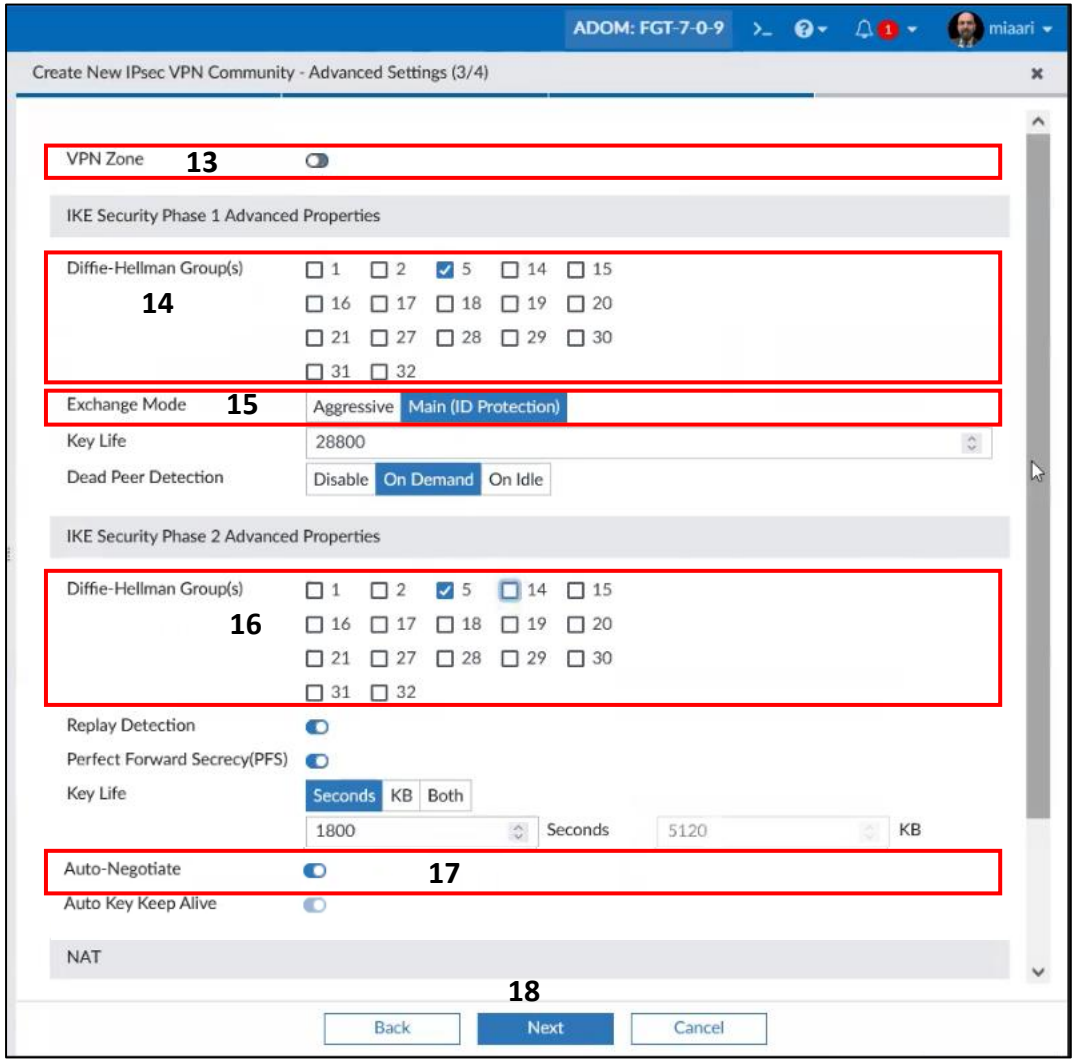
11. Choose the authentication algorithm for IPsec Security (Phase 2). This ensures the integrity and authenticity of the encrypted data packets.

"MD5" is selected as the authentication method.

12 After configuring the authentication and encryption settings, click the "Next" button at the bottom right to continue to the next step in the VPN community setup.

13. **VPN Zone:** This option allows you to assign the VPN to a specific zone. Zones are used to group multiple interfaces together and apply security policies. Enabling this can simplify policy management when multiple interfaces are involved.

"VPN Zone" is disabled



14. **Diffie-Hellman Group(s):** Select the Diffie-Hellman group(s) for key exchange during Phase 1. The selected group(s) determine the cryptographic strength.

groups "**5**" is selected. Group 5 is a 1536-bit key

15. **Exchange Mode:** Choose between "Aggressive" and "Main (ID Protection)" modes.

Aggressive Mode: Faster but less secure, revealing more information during the exchange.

Main Mode (ID Protection): More secure as it protects the identity of the peers during the exchange.

"Main (ID Protection)" is selected, providing more security.

16. **Diffie-Hellman Group(s):** Select the Diffie-Hellman group(s) for key exchange during Phase 2. This step is crucial for ensuring secure key exchanges during the ongoing IPsec sessions.

groups "**5**" is selected., similar to Phase 1.

Continue:

17. **Auto-Negotiate:** This option allows the VPN to automatically negotiate security associations (SAs) when required.

Auto-Negotiate is "enabled" , meaning the VPN will automatically negotiate connections as needed.

18. After configuring the advanced settings, click the "Next" button at the bottom right to continue to the final step in the VPN community setup.

❖ **Additional Settings:**

Replay Detection: This option (enabled in the image) helps protect against replay attacks by ensuring that old or duplicate packets are not accepted.

Perfect Forward Secrecy (PFS): Enabling PFS (which is turned on in the image) ensures that the keys used for encryption are not derived from the previous session keys, enhancing security.

Key Life: Specifies the lifetime of the keys for Phase 2. In the image, the key life is set to 1800 seconds (30 minutes), meaning the keys will be renegotiated after this period.

- **Security Considerations:**

  DES and MD5: Both DES encryption and MD5 authentication are outdated and considered insecure by today's standards. It would be more secure to use AES for encryption and SHA-256 or higher for authentication.

  Diffie-Hellman Group 5: While still in use, this group is also considered less secure compared to modern alternatives. Consider using a higher group (e.g., 14 or 19) for better security.

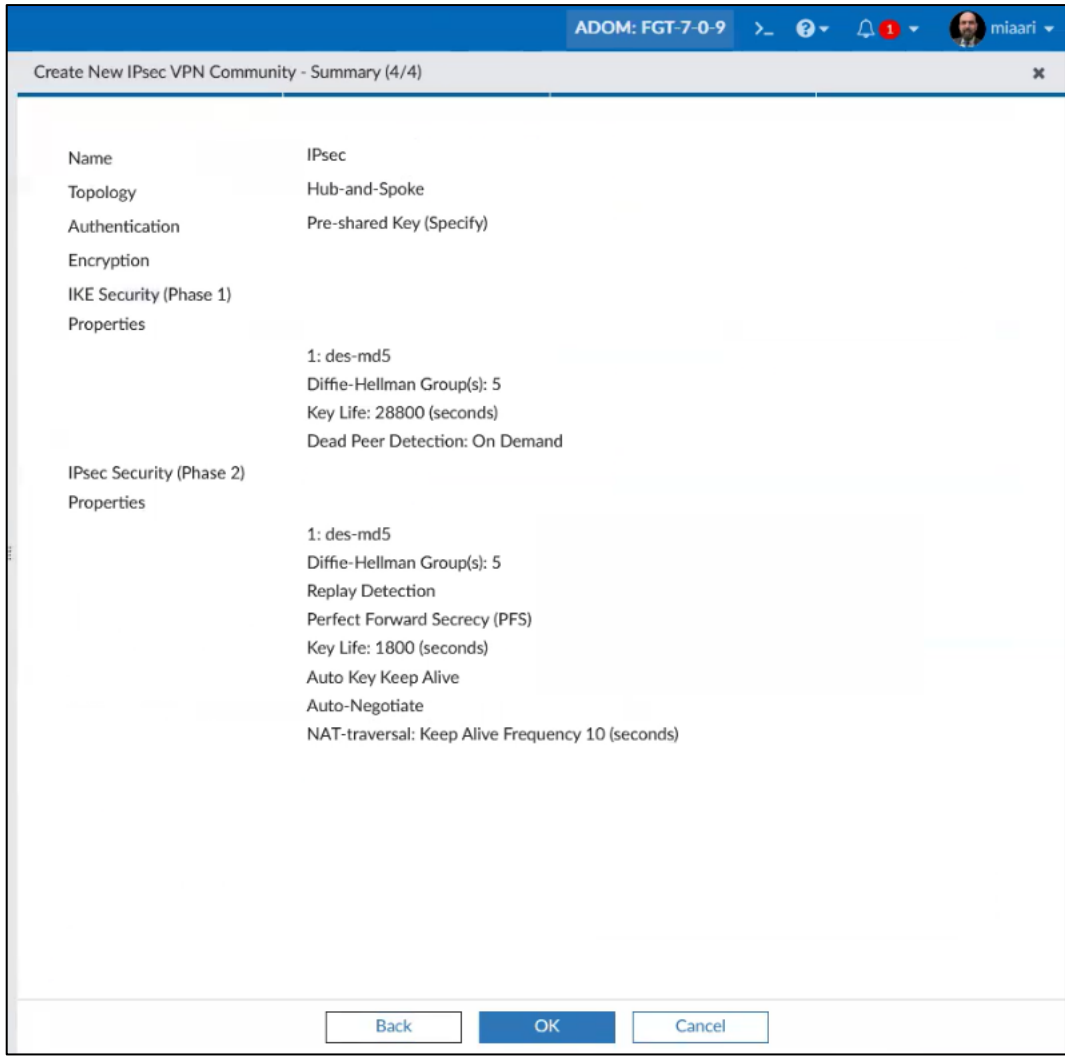
- **Configuration Appropriateness:**

  The configuration seems appropriate for a basic VPN setup, but for environments requiring strong security, it's recommended to update the cryptographic settings to more modern standards.

- **Potential for Improvement:**

  Upgrade Encryption and Authentication Algorithms: Using stronger algorithms like AES and SHA-256 would significantly enhance security.

  Reevaluate Diffie-Hellman Groups: Consider using more secure groups to ensure the integrity and security of the key exchange process.



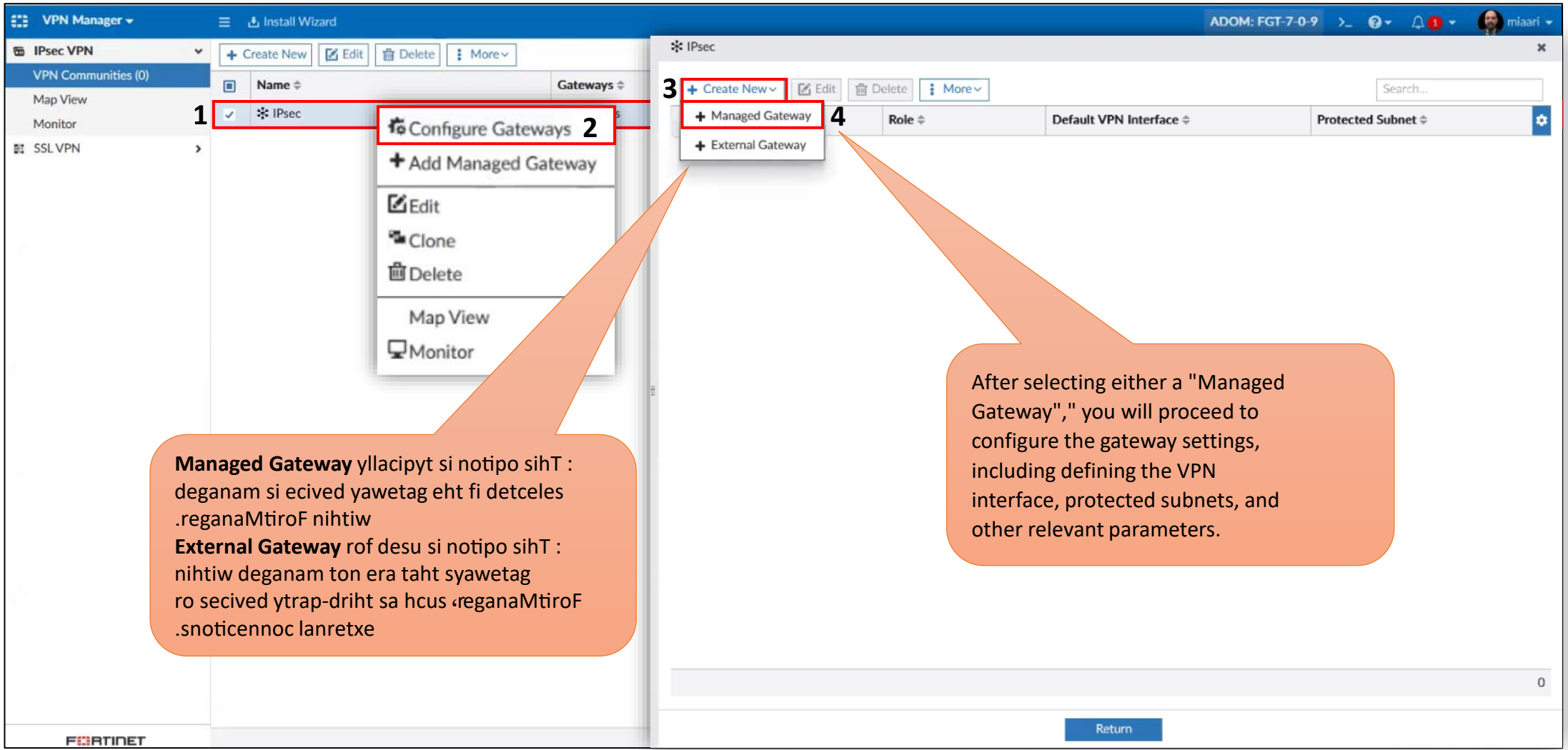
- To add Gateway for “Head Quarter”:

1. Select the newly created VPN community named "IPsec" by checking the box next to it. right-click on it to open the context menu.

2. Choose the "Configure Gateways" option from the dropdown menu. This will allow you to set up and manage the gateways for this VPN community.

3. Click on the "Create New" button to add a new gateway to the VPN community.

4. From the dropdown menu, select the type of gateway you want to add: "Managed Gateway" is selected.



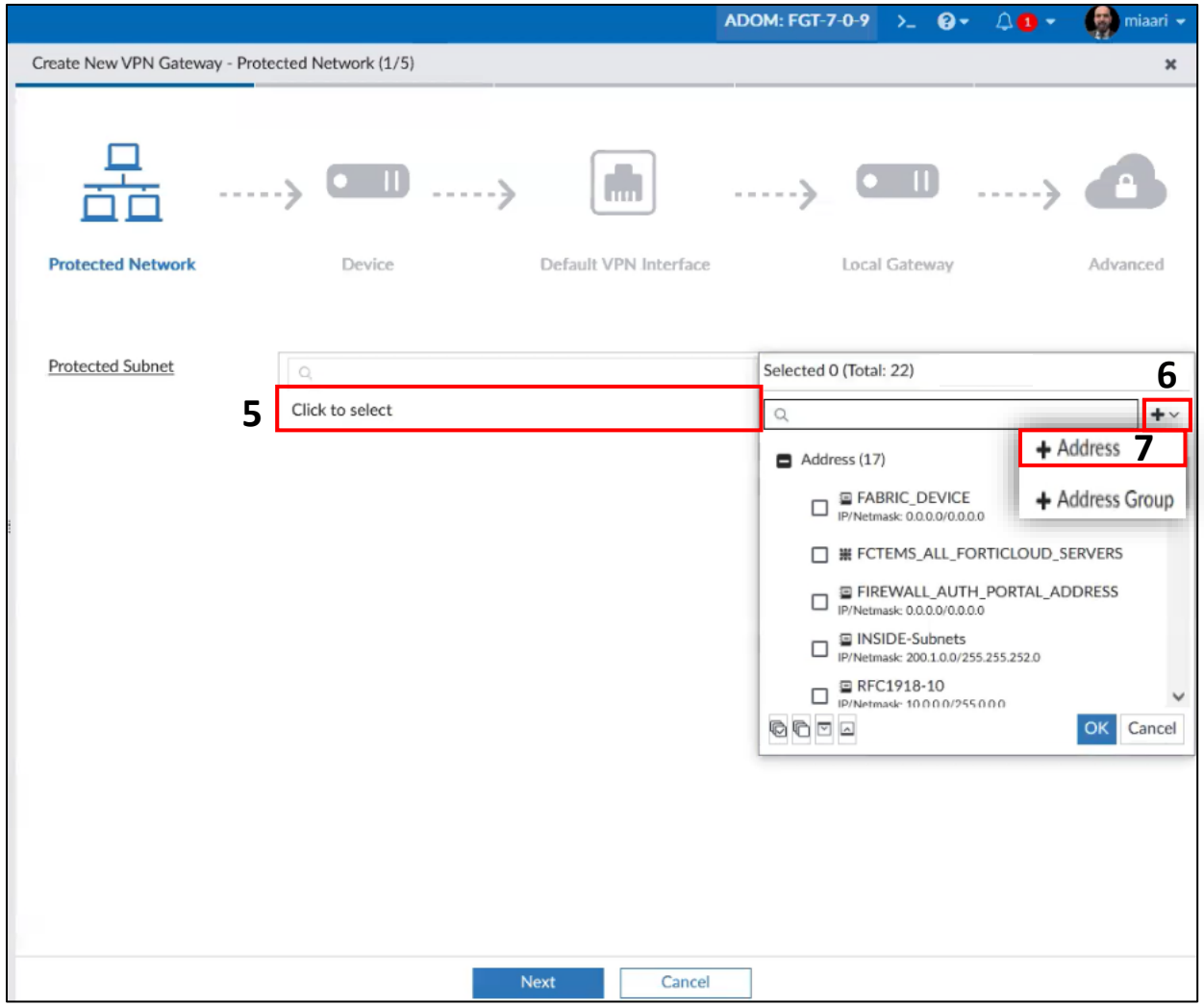
5. In the "Protected Subnet" field, click on the box labeled "Click to select" to open the list of available subnets.

   A dropdown list will appear, showing all the predefined addresses (subnets) that are available for selection. You can scroll through the list to find and select the desired subnet(s).

6. If the required subnet is not listed, click on the "+" button next to the address field. This will provide options to either:

   - **+ Address:** Create a new address by defining a specific IP range or subnet.
   - **+ Address Group:** Create a new group that can contain multiple addresses or subnets.

7. Select "Address" .



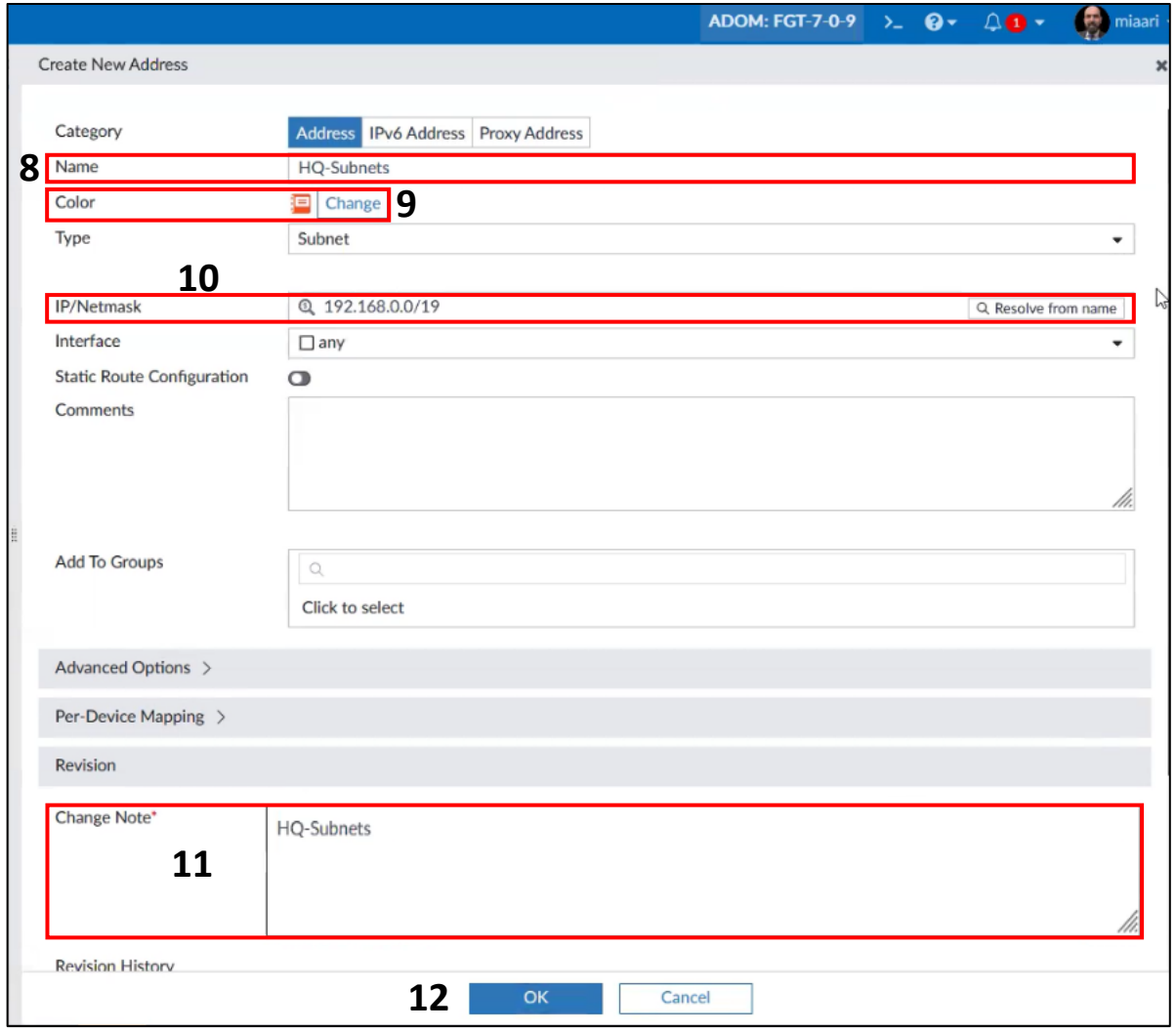
8. In the "Name" field, enter a descriptive name for the new address, "HQ-Subnets" is used, which indicates that this address will represent the subnets for the headquarters.

9. Click on the "Change" button next to the "Color" field to assign a color to the address. This helps in visually distinguishing it from other addresses in FortiManager.

10. In the "IP/Netmask" field, enter the subnet that this address will represent. For example, Summarized address (192.168.10.0/24, 192.168.20.0/24) , "192.168.0.0/19" is used. This defines the range of IP addresses that belong to this subnet.

11. In the "Change Note" field, provide a brief description or note about this change, such as "HQ-Subnets," to document why this address was created.

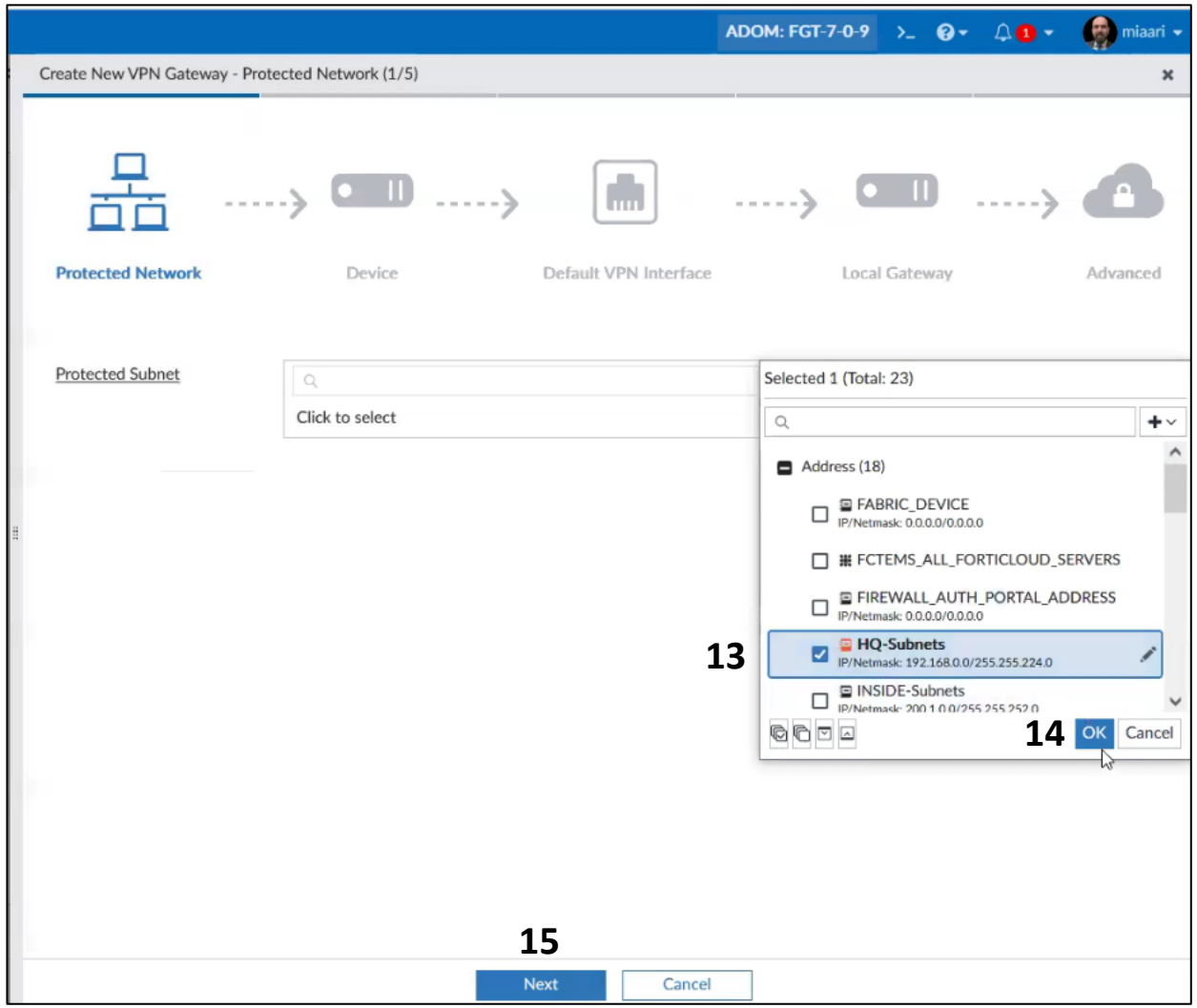
12. Once all necessary information is entered, click "OK" to save the new address. This action will close the address creation window and add the new subnet to the list of available addresses.



13. Back in the "Create New VPN Gateway" window under "Protected Network", click on the "Click to select" field to open the list of available addresses.Find and select the newly created address (e.g., "HQ-Subnets").

14. After selecting the new address, click "OK" to confirm your selection. This action will close the address selection window and return you to the VPN Gateway configuration screen.

15. With the protected subnet selected, click "Next" at the bottom of the window to continue configuring the VPN Gateway.



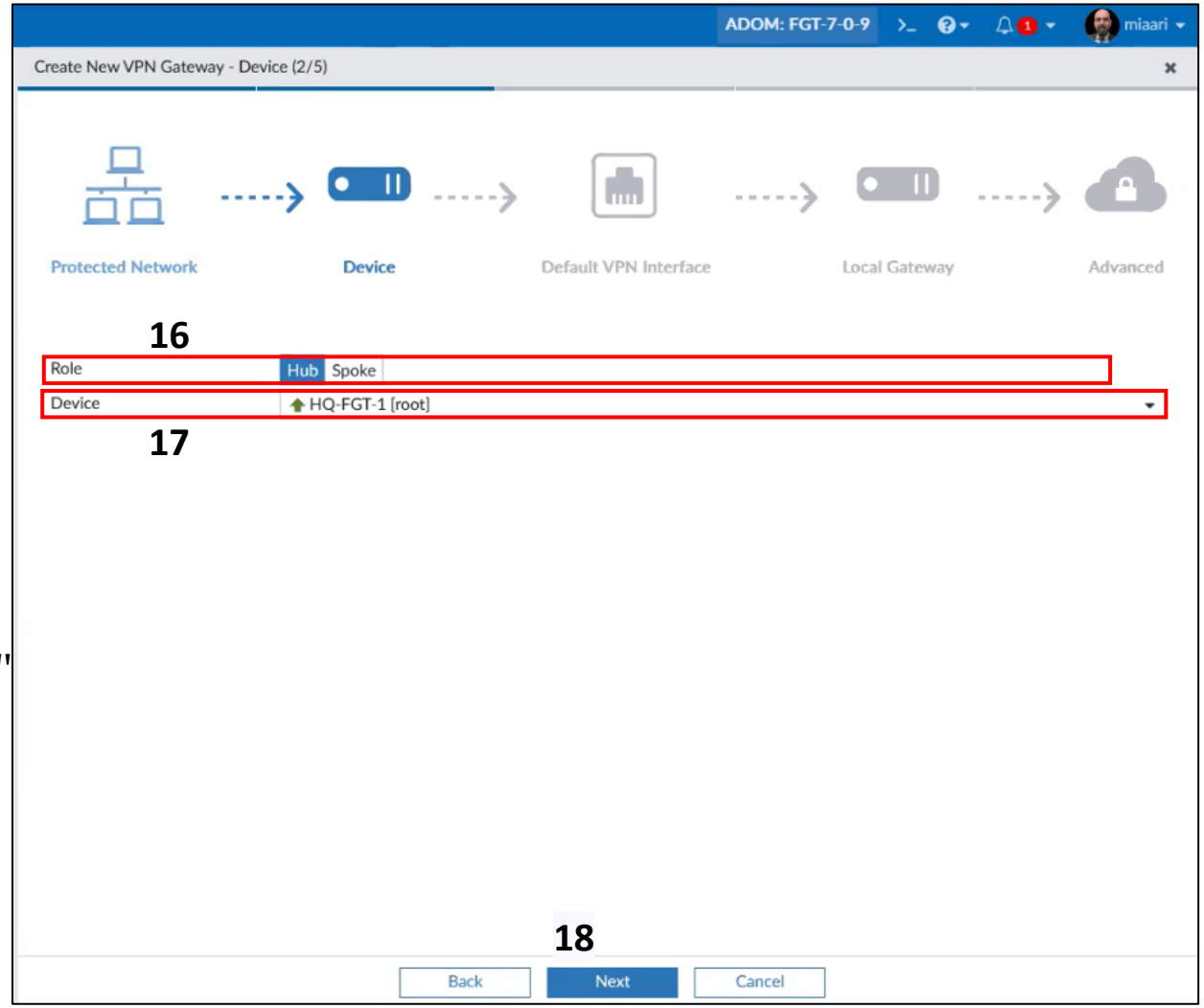
16. In the "Role" section, choose whether the device will act as a **Hub** or a **Spoke** in the VPN topology.

"Hub" is selected, meaning that this device will serve as the central point in a Hub-and-Spoke VPN topology, where all spoke devices (branches or remote sites) will connect to this hub.

17. In the "Device" section, choose the specific device that will play the selected role (Hub or Spoke).

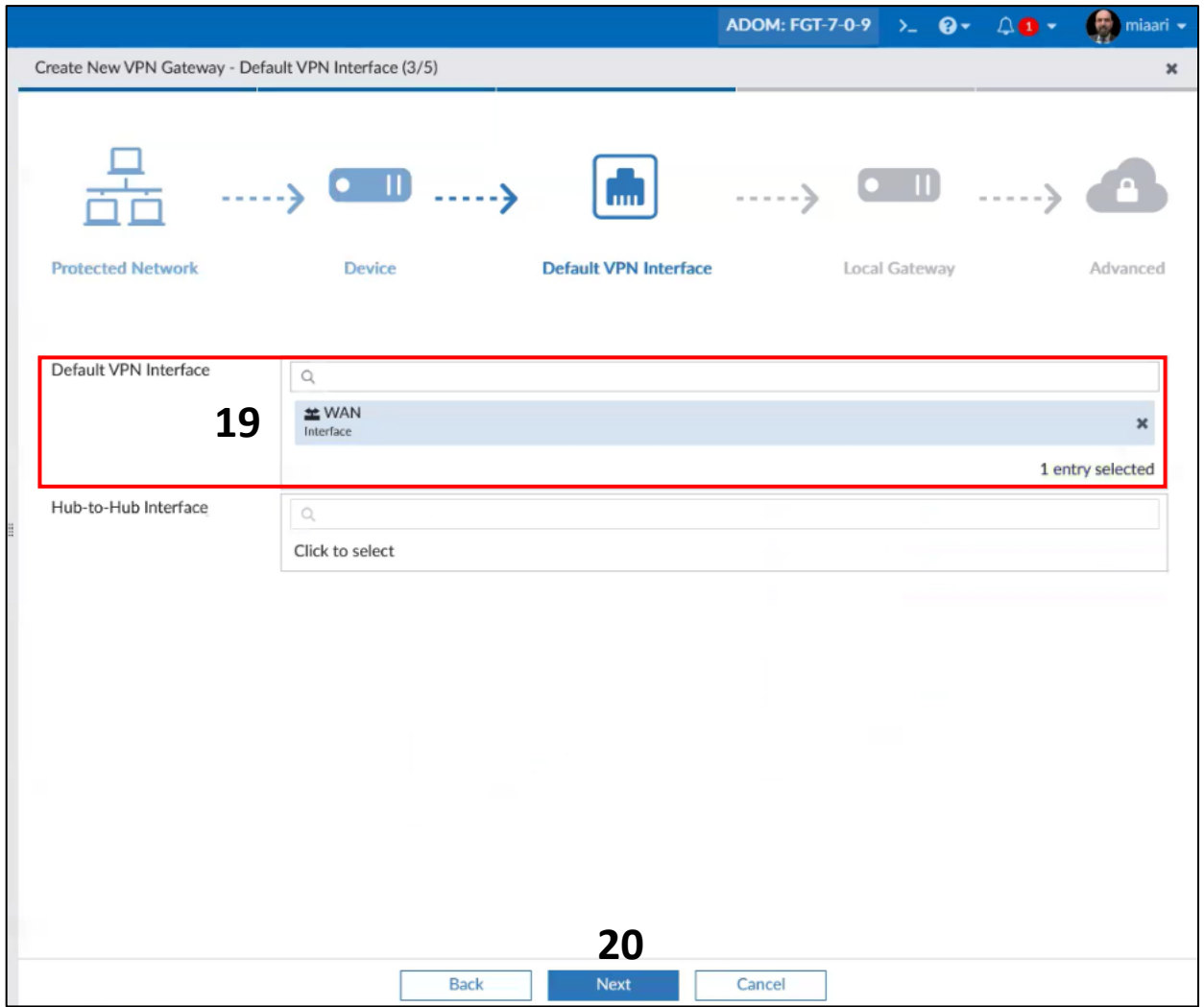
"HQ-FGT-1 [root]" is selected, which likely represents a FortiGate device designated as the headquarters' main firewall or VPN gateway.

18. Once you have selected the role and device, click the "Next" button at the bottom of the window to continue with the VPN Gateway configuration process.



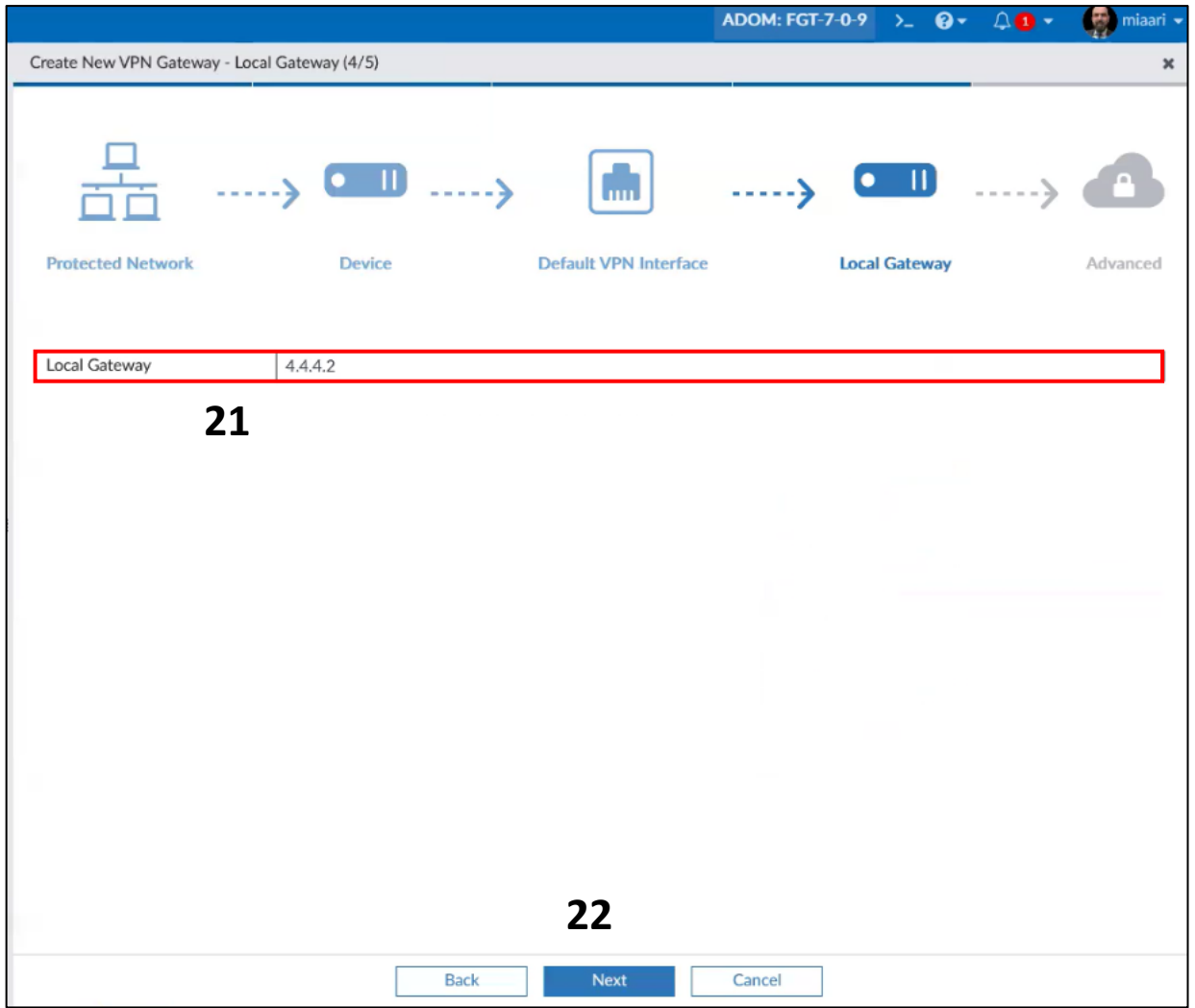
19. In the "Default VPN Interface" section, click on the field to display the list of available interfaces . From the list, select the appropriate interface that will be used for the VPN connection . The "WAN" interface is selected, which is typically the interface connected to the internet.

20. Once the Default VPN Interface is selected, click the "Next" button at the bottom of the window to continue with the VPN Gateway configuration.



21. In the "Local Gateway" section, enter the IP address that will be used as the local gateway for the VPN. This is the IP address on the local network that the VPN will use to establish the connection . The IP address "4.4.4.2" is entered as the Local Gateway.

22. After entering the Local Gateway IP, click the "Next" button at the bottom of the window to continue with the VPN Gateway setup.



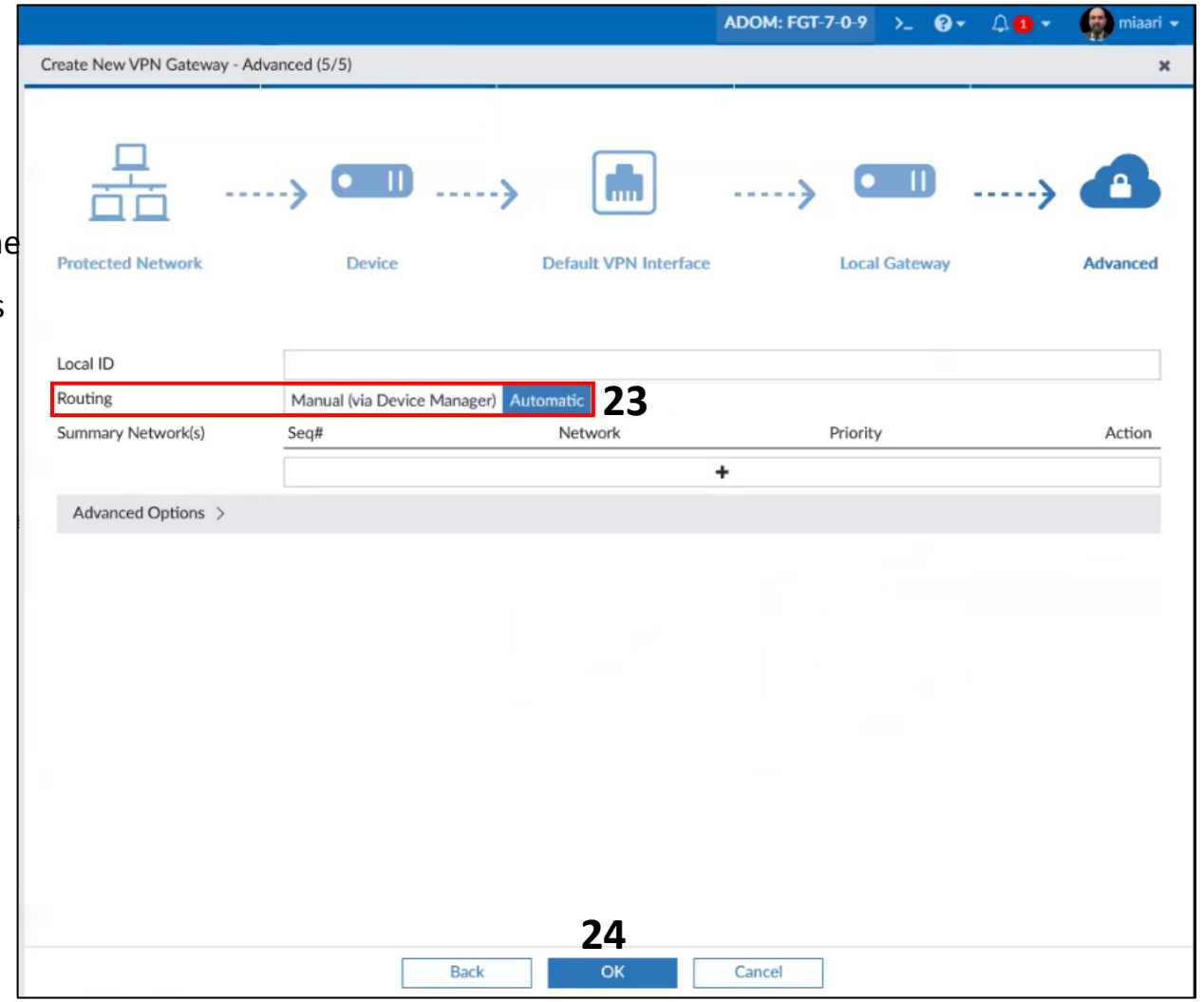
23. In the "Routing" section, you have the option to select how the routing will be managed for the VPN:

- **Manual (via Device Manager):** This option allows you to manually configure routing through the Device Manager. You would need to set up the necessary routing policies manually within the device configurations.
- **Automatic:** This option lets FortiManager automatically handle the routing configurations for the VPN. It simplifies the process by automatically setting up the necessary routes based on the network and device settings.

"Automatic" is selected, meaning that FortiManager will automatically configure the routing needed for this VPN Gateway.

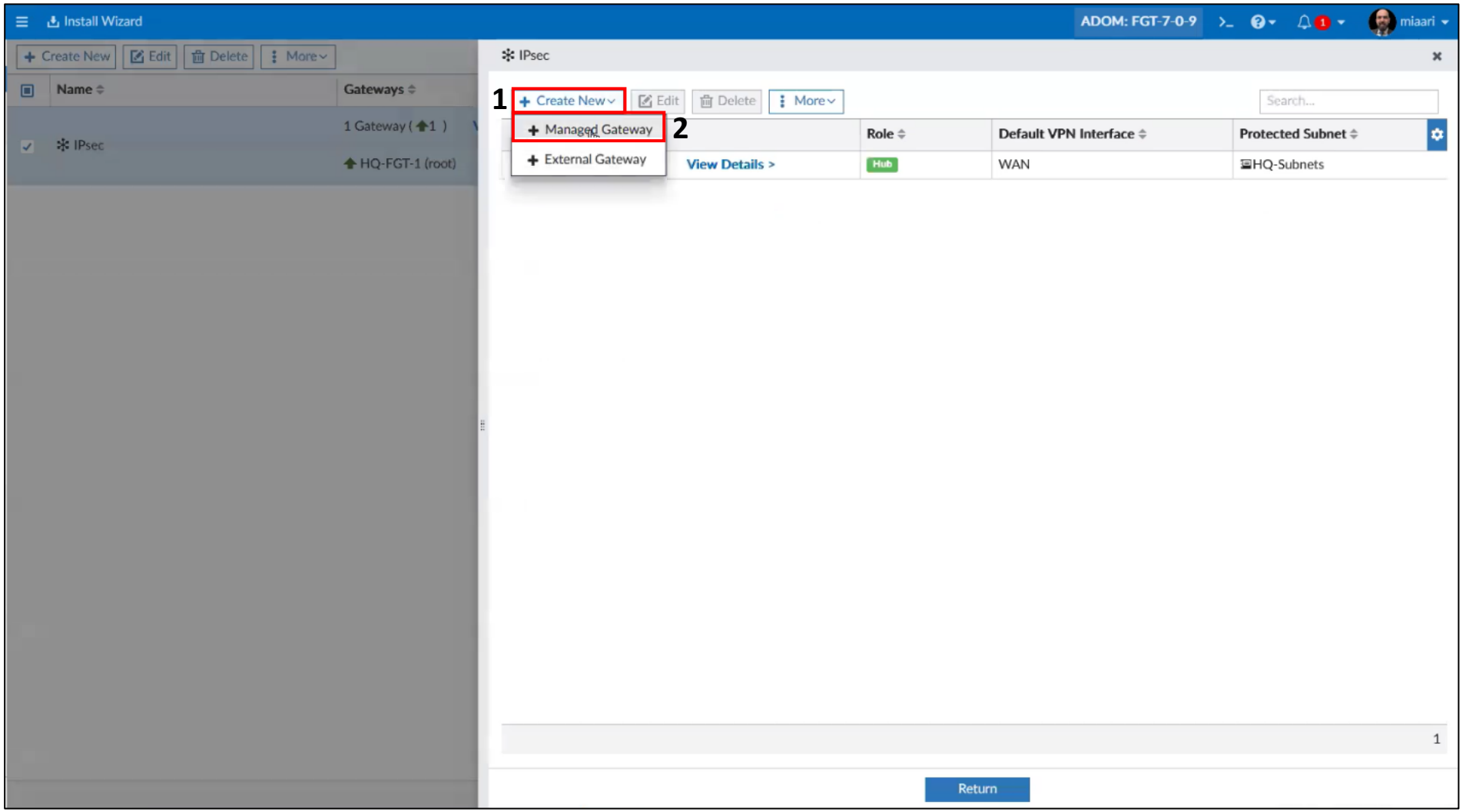
❖ If you want to add specific networks to the summary, you can do so in the "Summary Network(s)" section. However, no specific summary networks are defined, which is typical if you want the automatic routing to handle everything.

24. Once the routing method is selected and any necessary network summaries are reviewed or added, click the "OK" button at the bottom of the window to finalize the VPN Gateway configuration. Clicking "OK" completes the setup process and applies the configurations.



- To create a managed gateway for a branch-1 :

1. Click on the "Create New" .
2. "Managed Gateway" is selected.



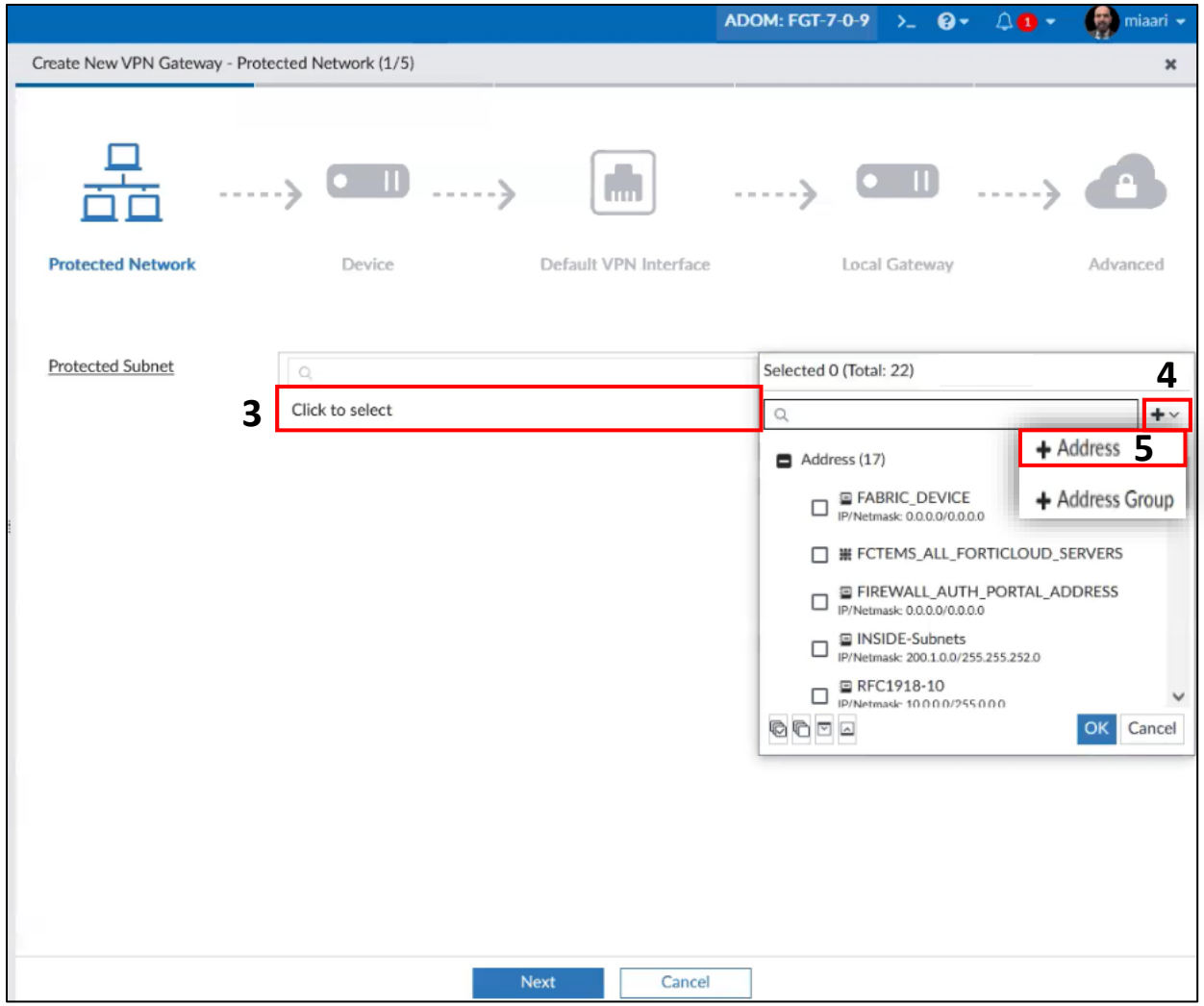
3. In the "Protected Subnet" field, click on the box labeled "Click to select" to open the list of available subnets.

   A dropdown list will appear, showing all the predefined addresses (subnets) that are available for selection. You can scroll through the list to find and select the desired subnet(s).

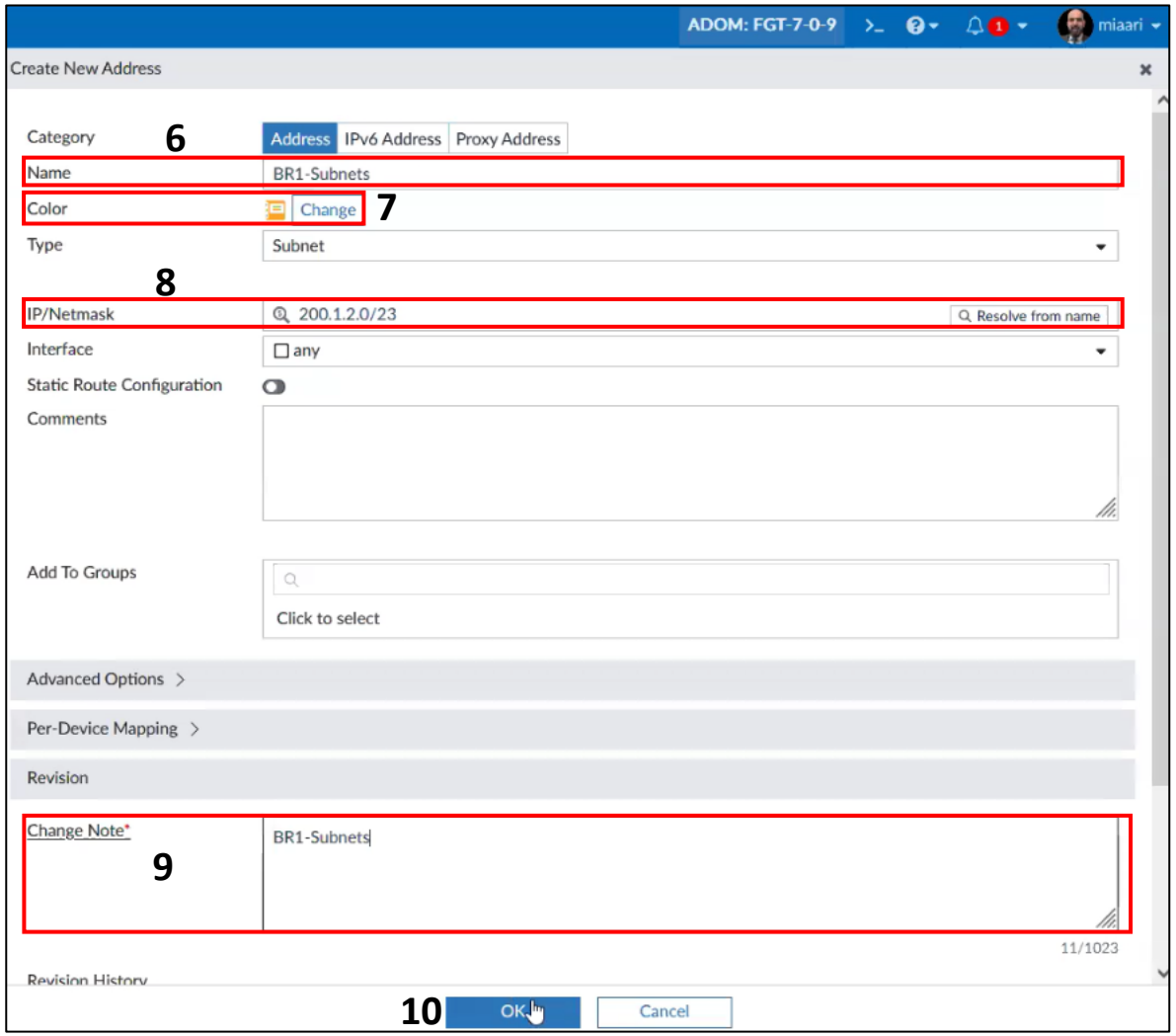
4. If the required subnet is not listed, click on the "+" button next to the address field. This will provide options to either:

   - **+ Address:** Create a new address by defining a specific IP range or subnet.
   - **+ Address Group:** Create a new group that can contain multiple addresses or subnets.

5. Select "Address" .



- To create a managed gateway for a branch-1 : Be mindful of the differences



6. In the "Name" field, enter a descriptive name for the new address. " BR1-Subnets " is used.
7. Click on the "Change" .
8. In the "IP/Netmask" field, enter Summarized address (200.1.2.0/24, 200.1.3.0/24) , “200.1.2.0/23" is used.
9. Enter "Change Note", such as " BR1-Subnets " .
10. Click on "OK" .

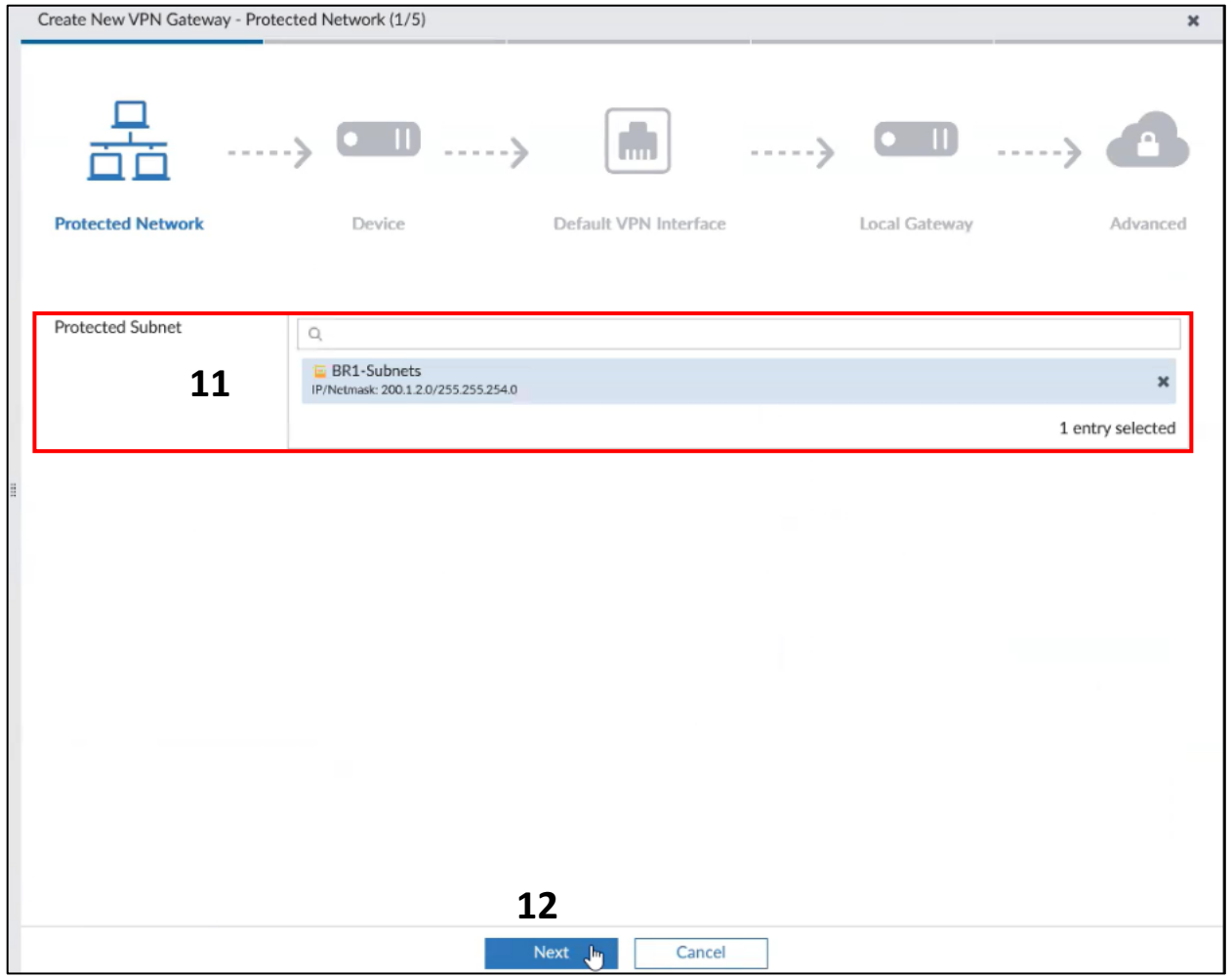
11. Back in the "Create New VPN Gateway" window under "Protected Network", Find and select the newly created address (e.g., “BR1-Subnets").

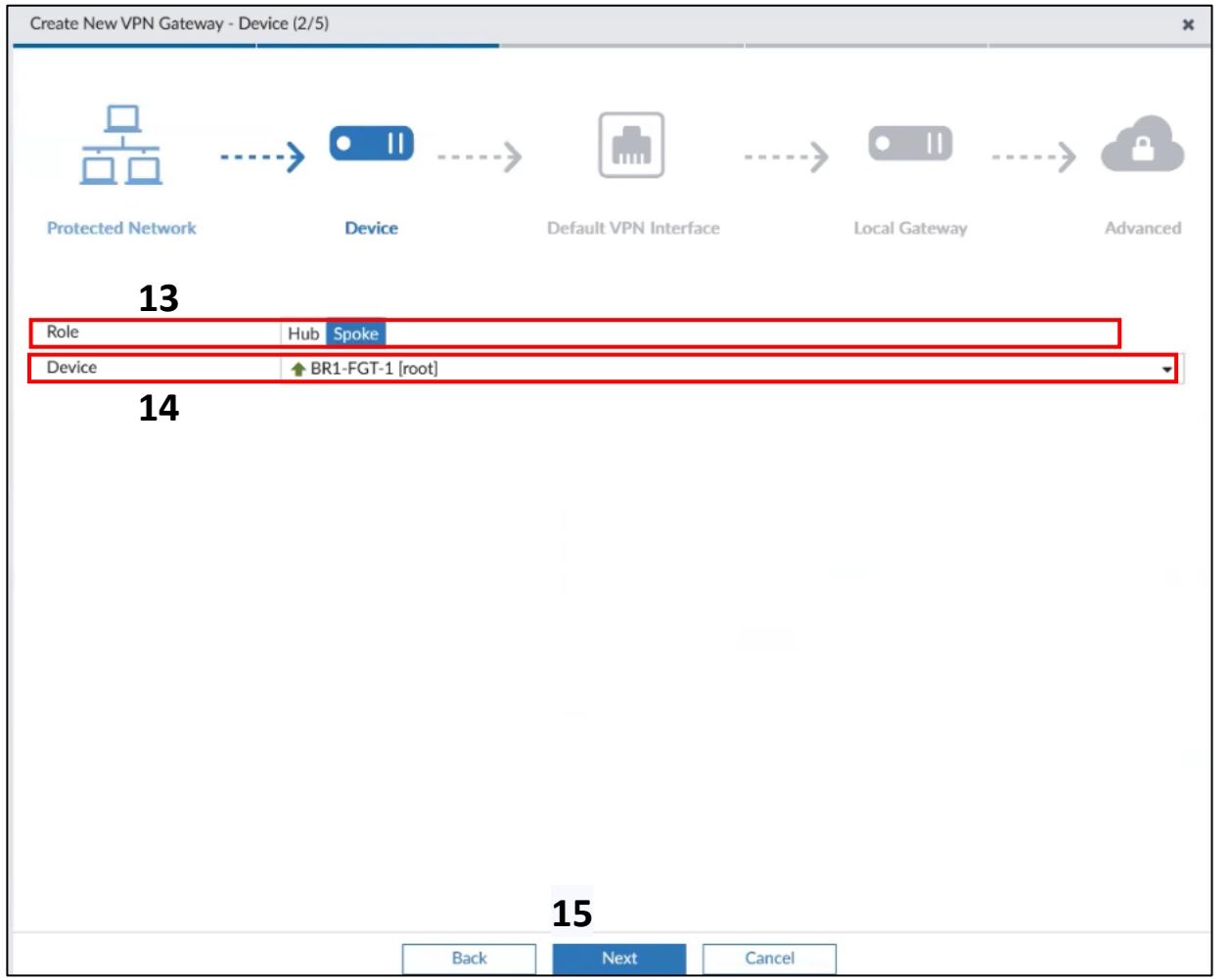
12. Click on "Next" .

13. Select “spoke”.

14. “BR1-FGT-1 [root]” is selected

15. Click the “Next”.



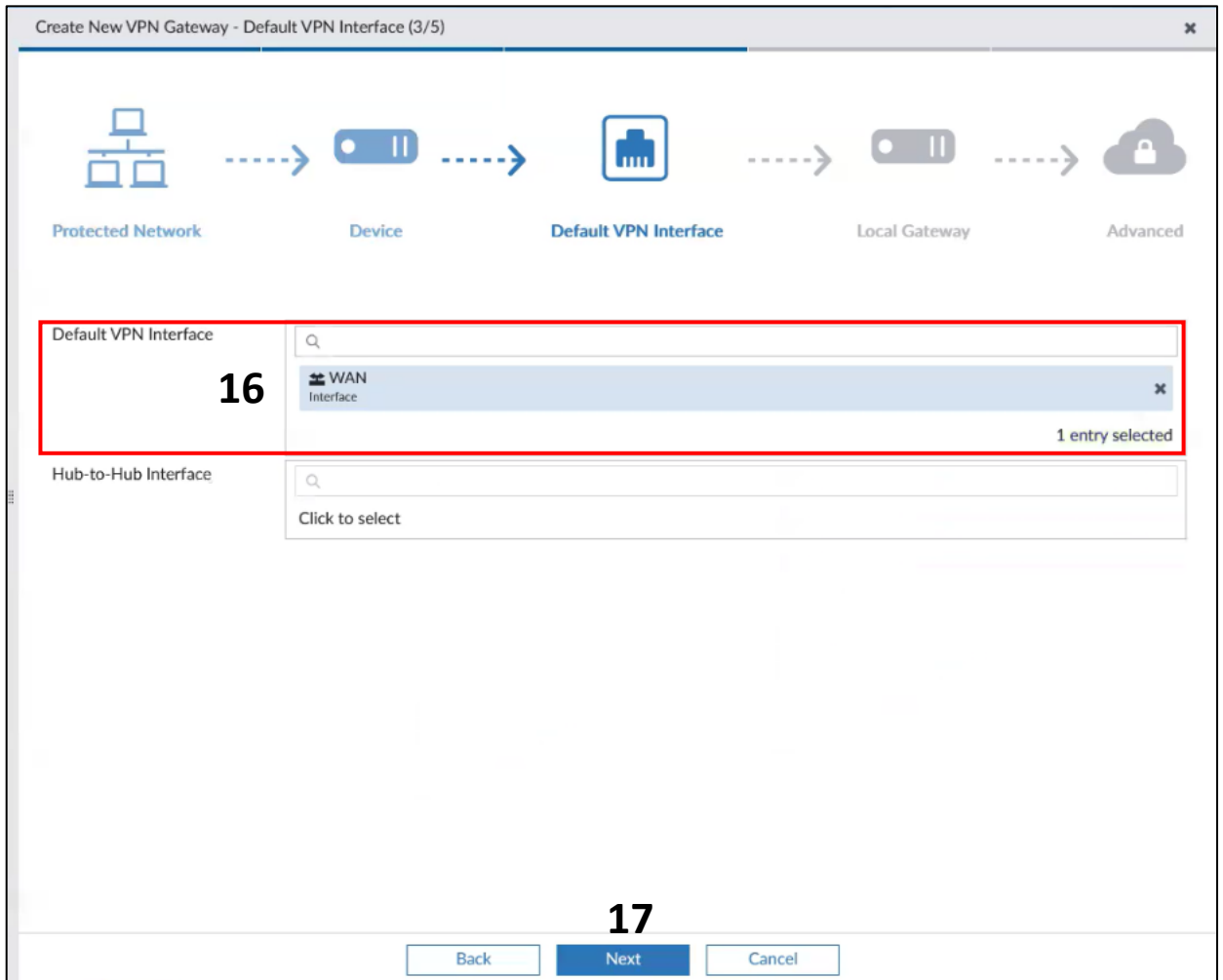


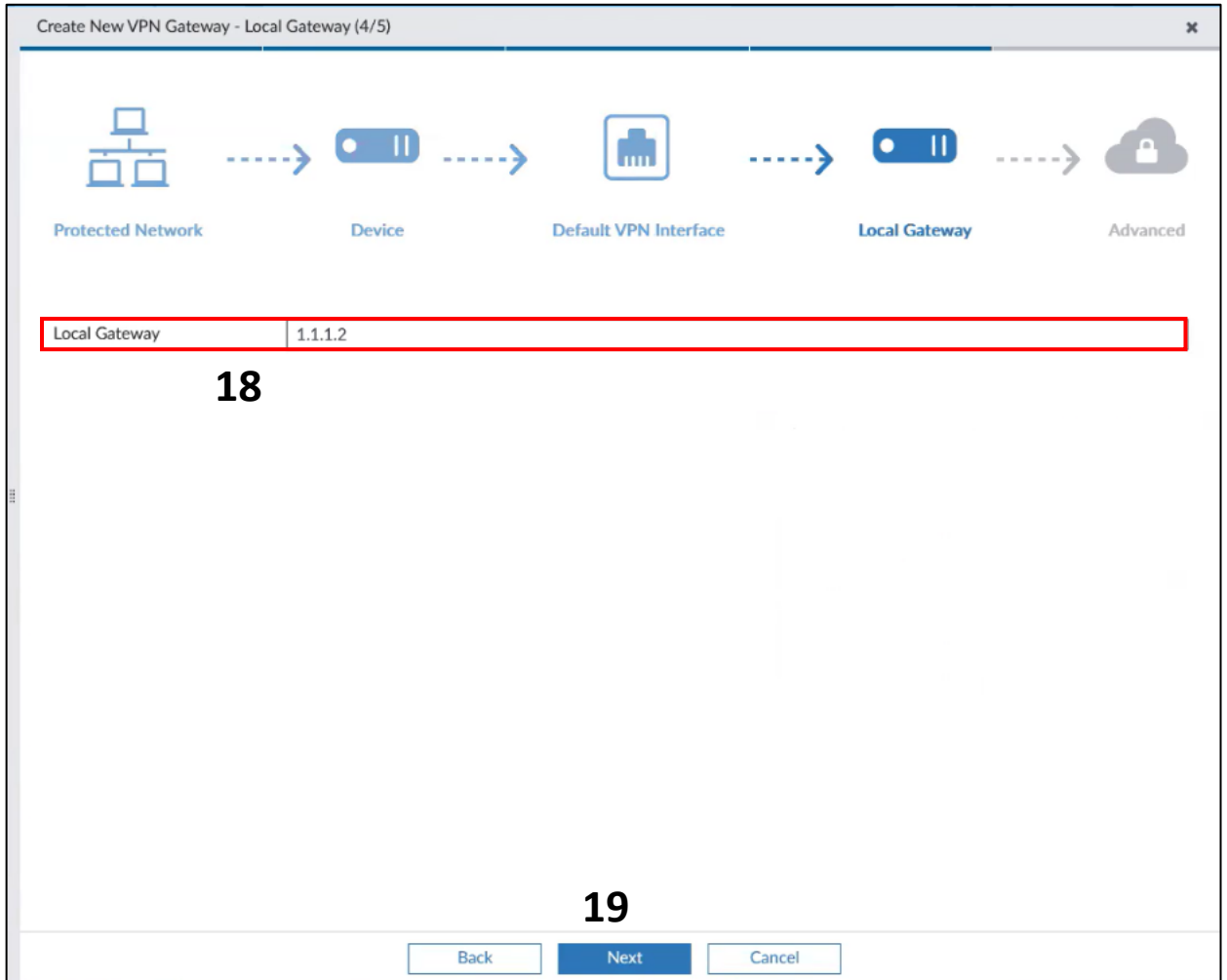
16. The "WAN" interface is selected, which is typically the interface connected to the internet.

17. Click the "Next" .

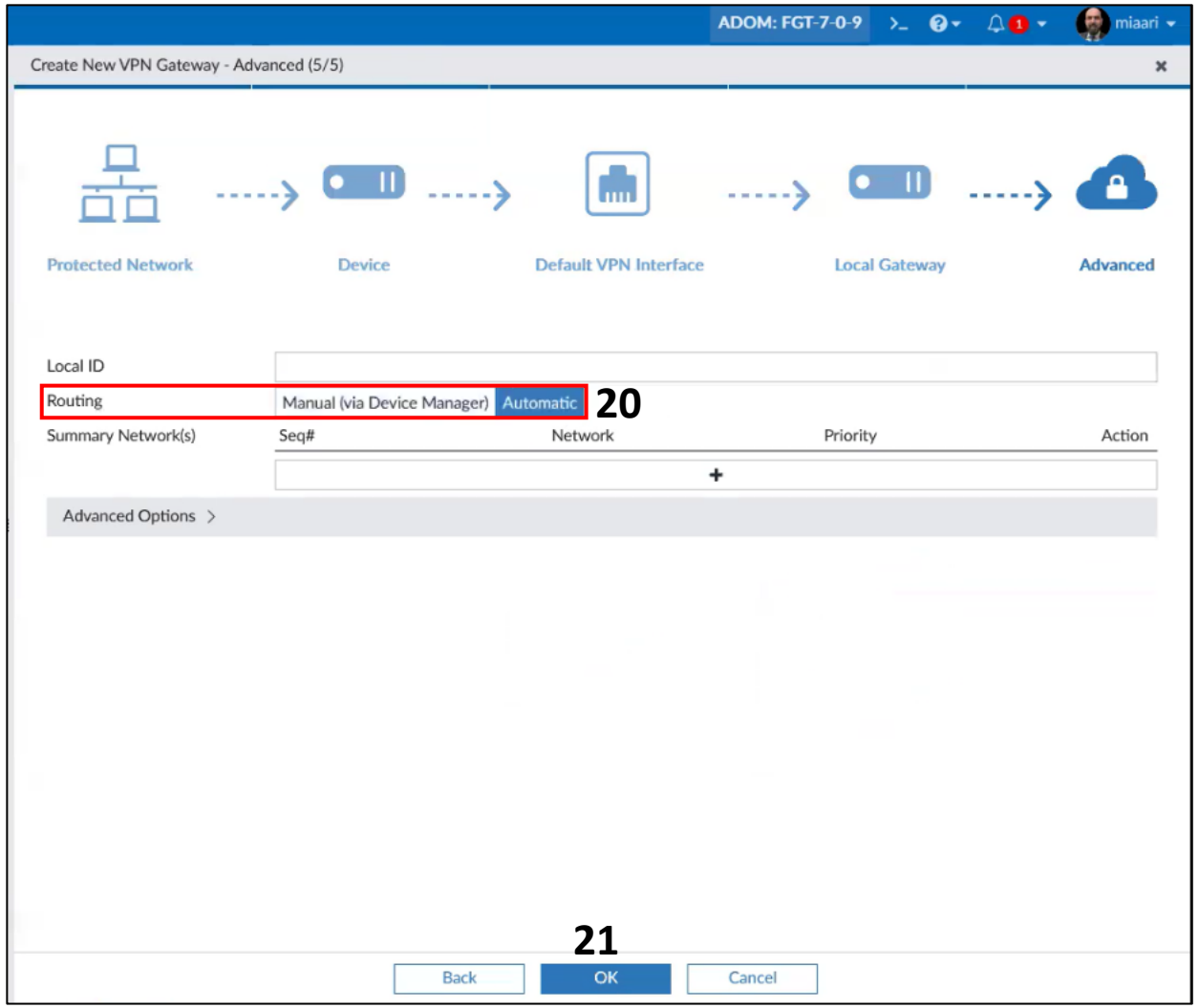
18. The IP address “1.1.1.2" is entered as the Local Gateway.

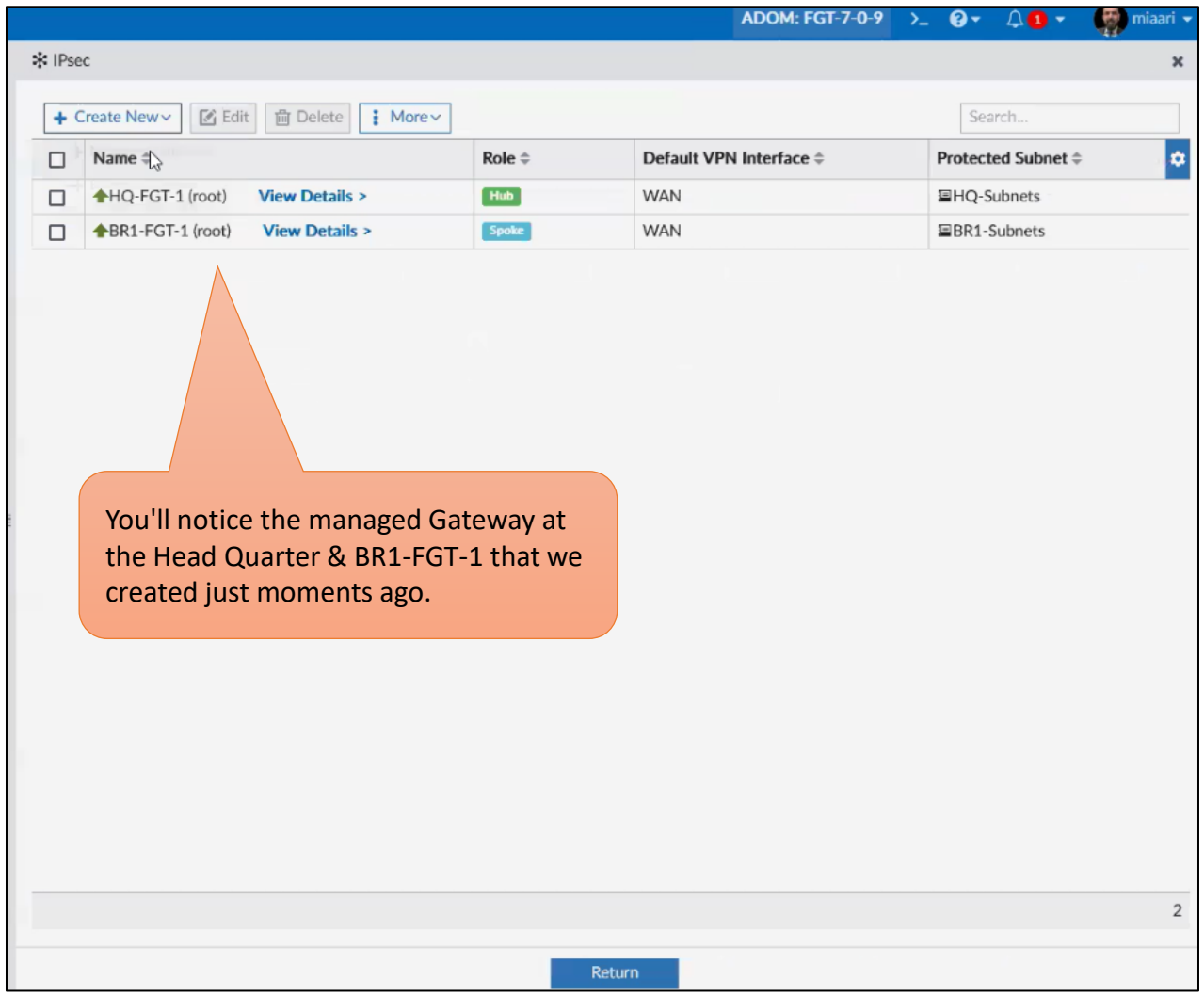
19. Click the "Next" .





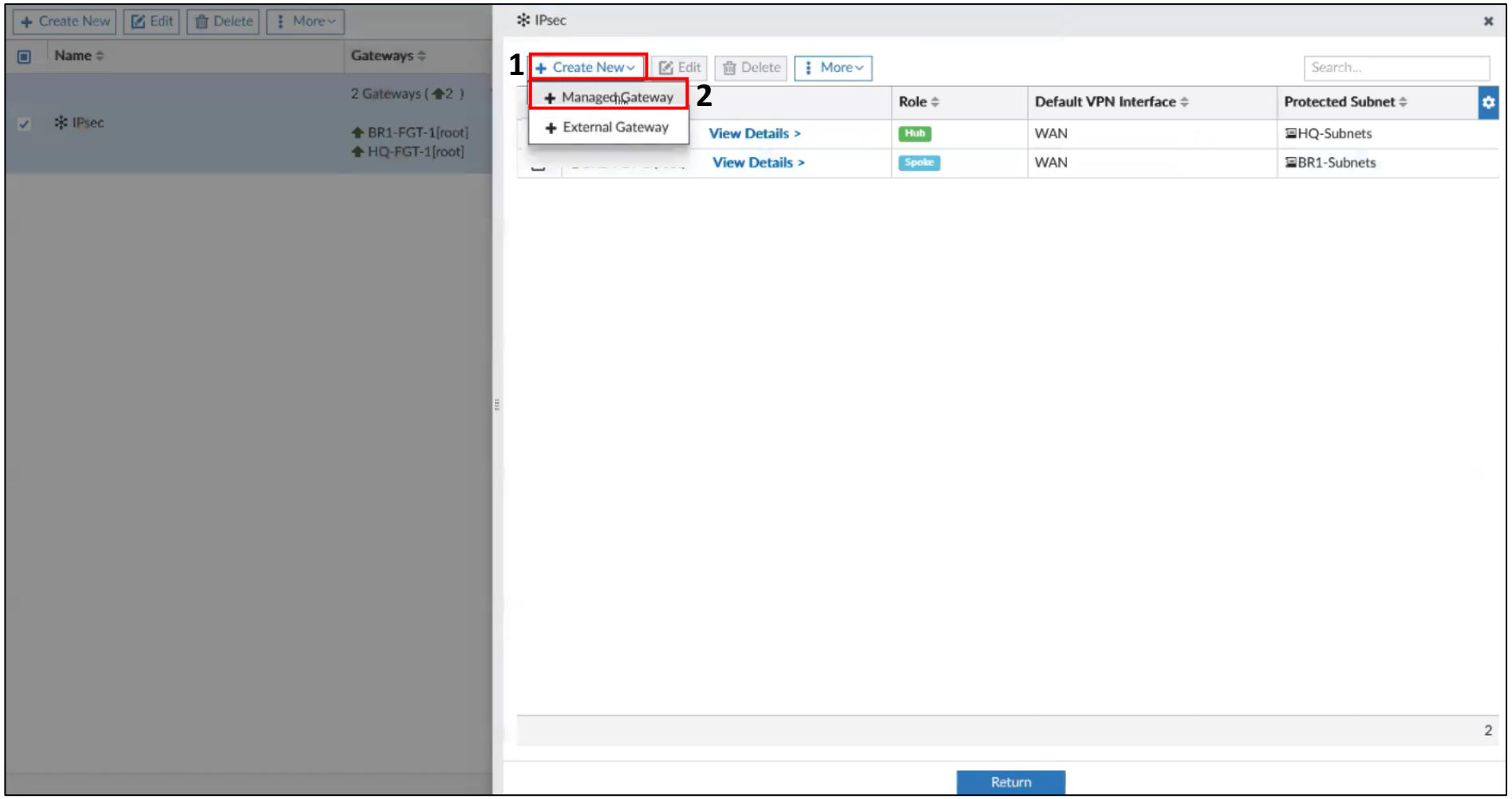
20. "Automatic" is selected.
21. Click the "OK" .



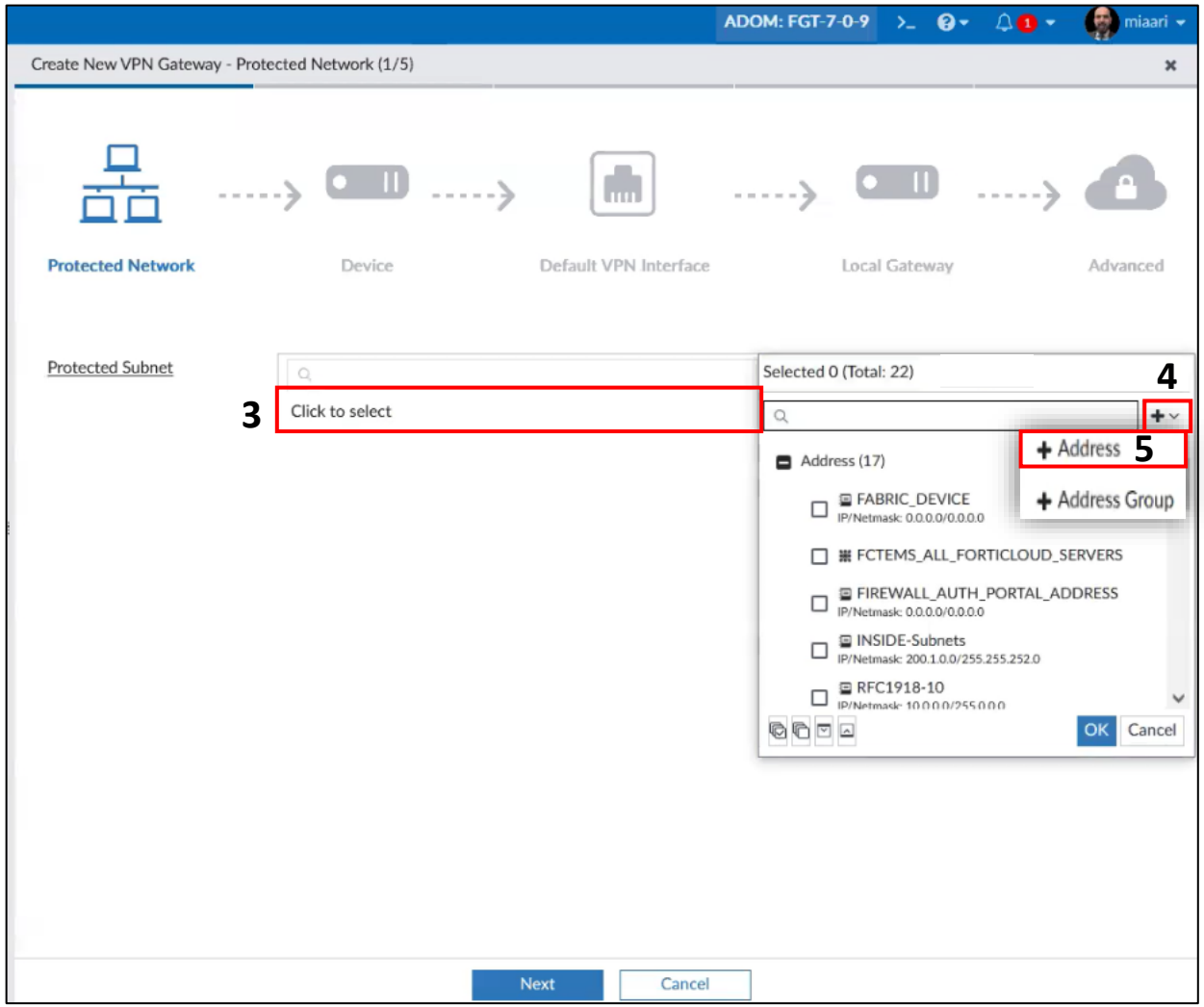


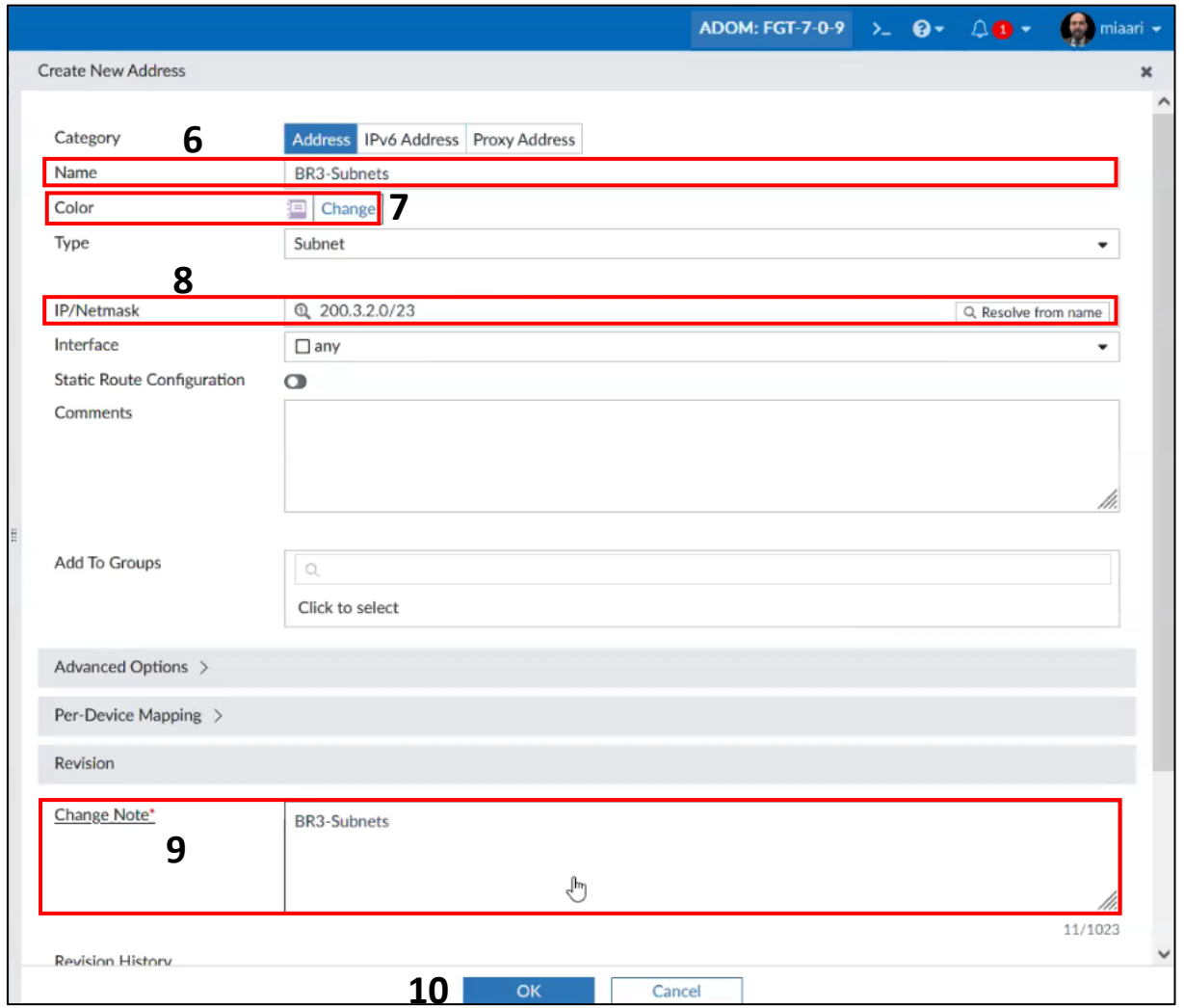
- To create a managed gateway for a branch-3 :

1. Click on the "Create New" .
2. "Managed Gateway" is selected.



3. Click on the box labeled "Click to select" to open the list of available subnets.
4. Click on the "+" button next to the address field.
5. Select "Address" .
6. In the "Name" field, enter a descriptive name for the new address. " BR3-Subnets " is used.
7. Click on the "Change“ and select color .
8. In the "IP/Netmask" field, enter Summarized address (200.3.2.0/24, 200.3.3.0/24) , “200.3.2.0/23" is used.
9. Enter "Change Note", such as “BR3-Subnets" .
10. Click on "OK" .





11. Back in the "Create New VPN Gateway" window under "Protected Network",

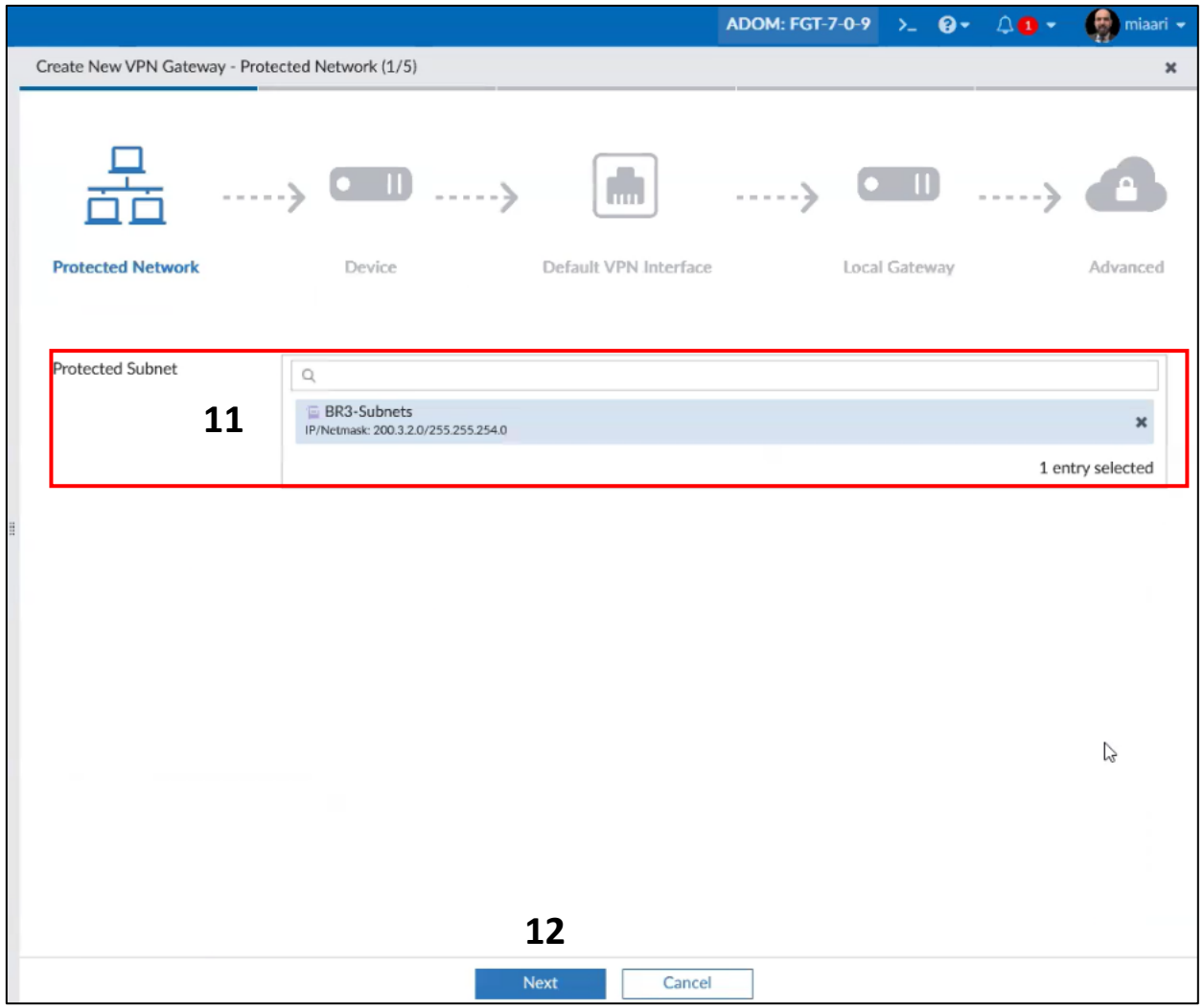
Find and select the newly created address (e.g., “BR3-Subnets").

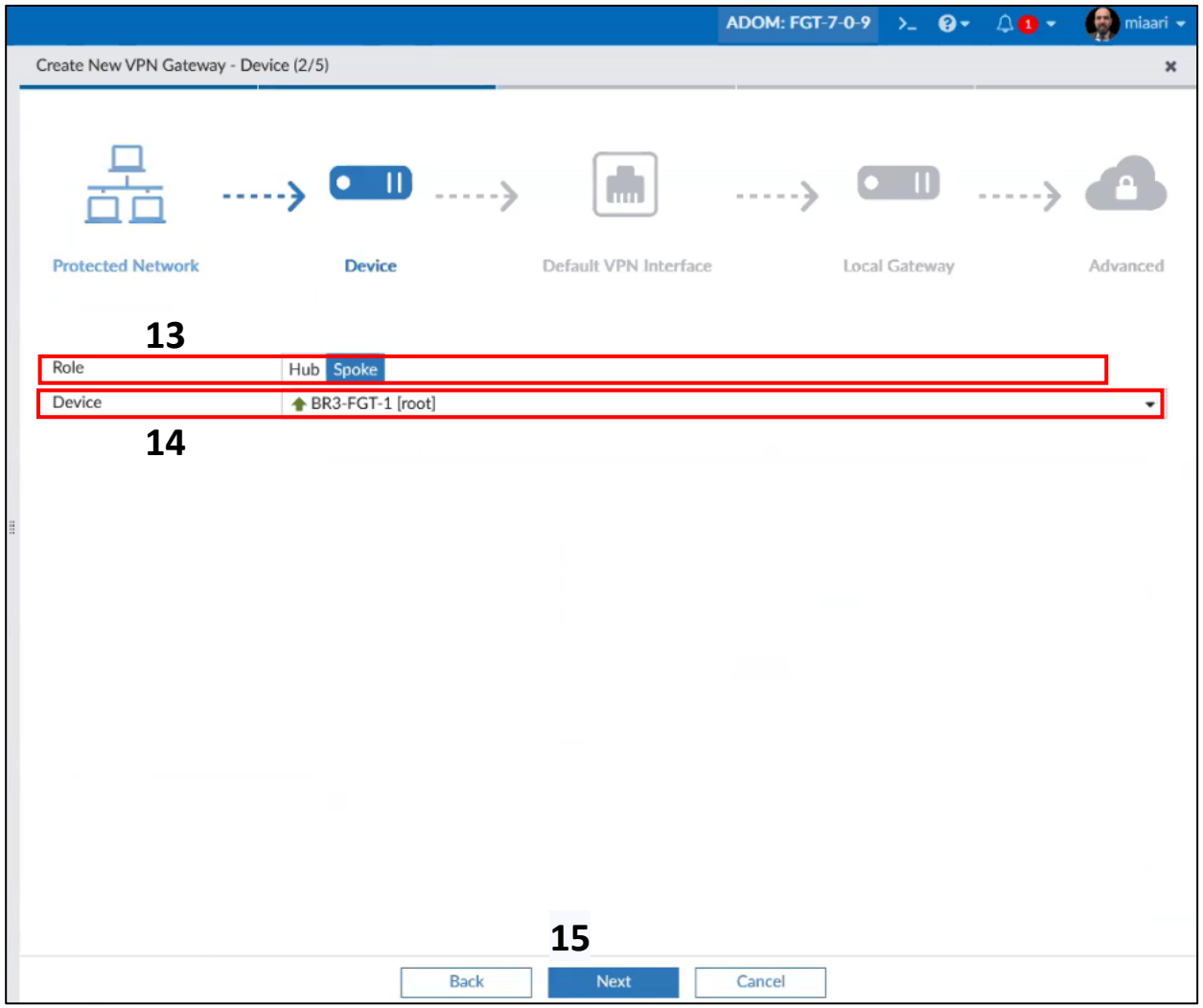
12. Click on "Next" .

13. Select “spoke”.

14. “BR3-FGT-1 [root]” is selected

15. Click the “Next”.



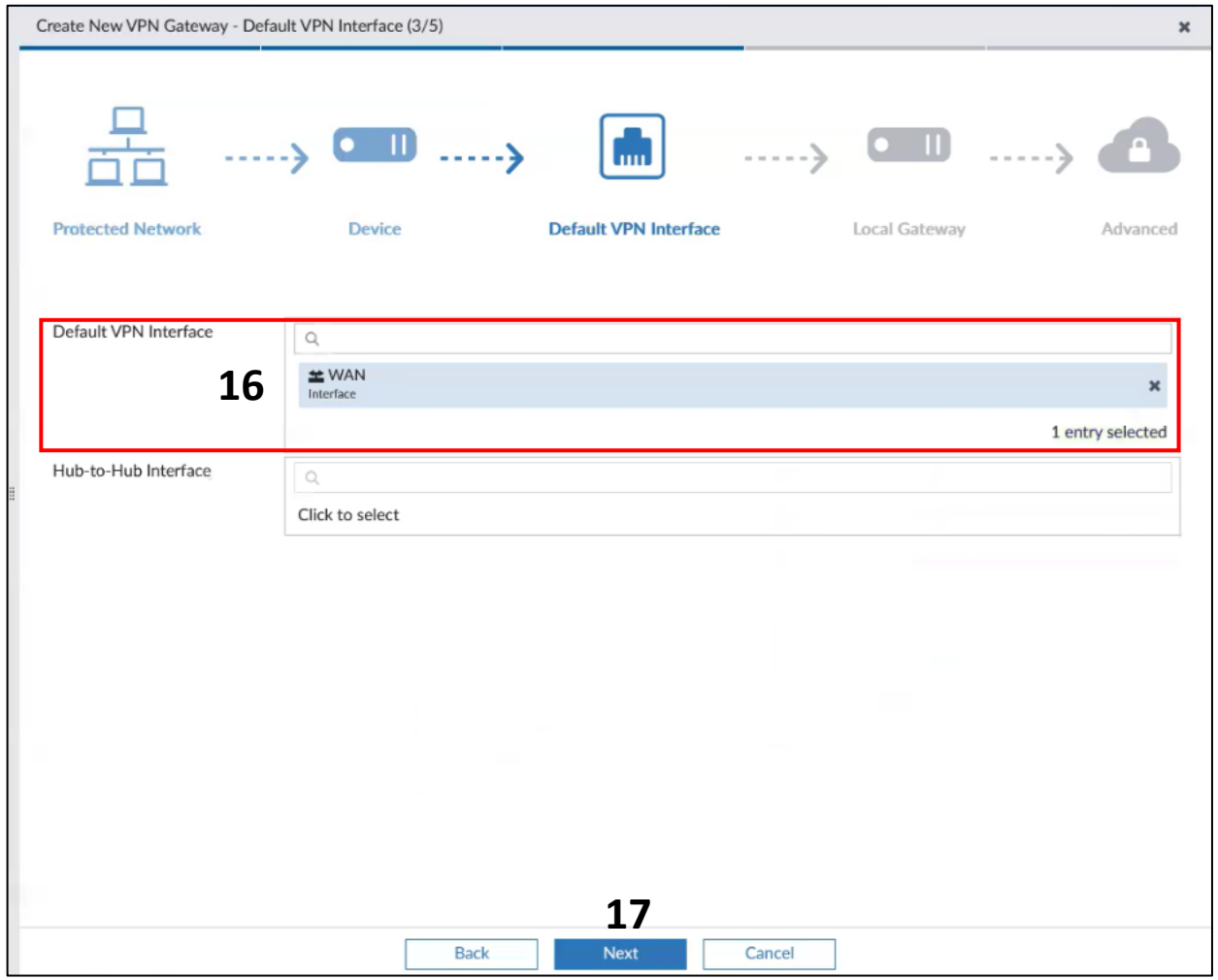


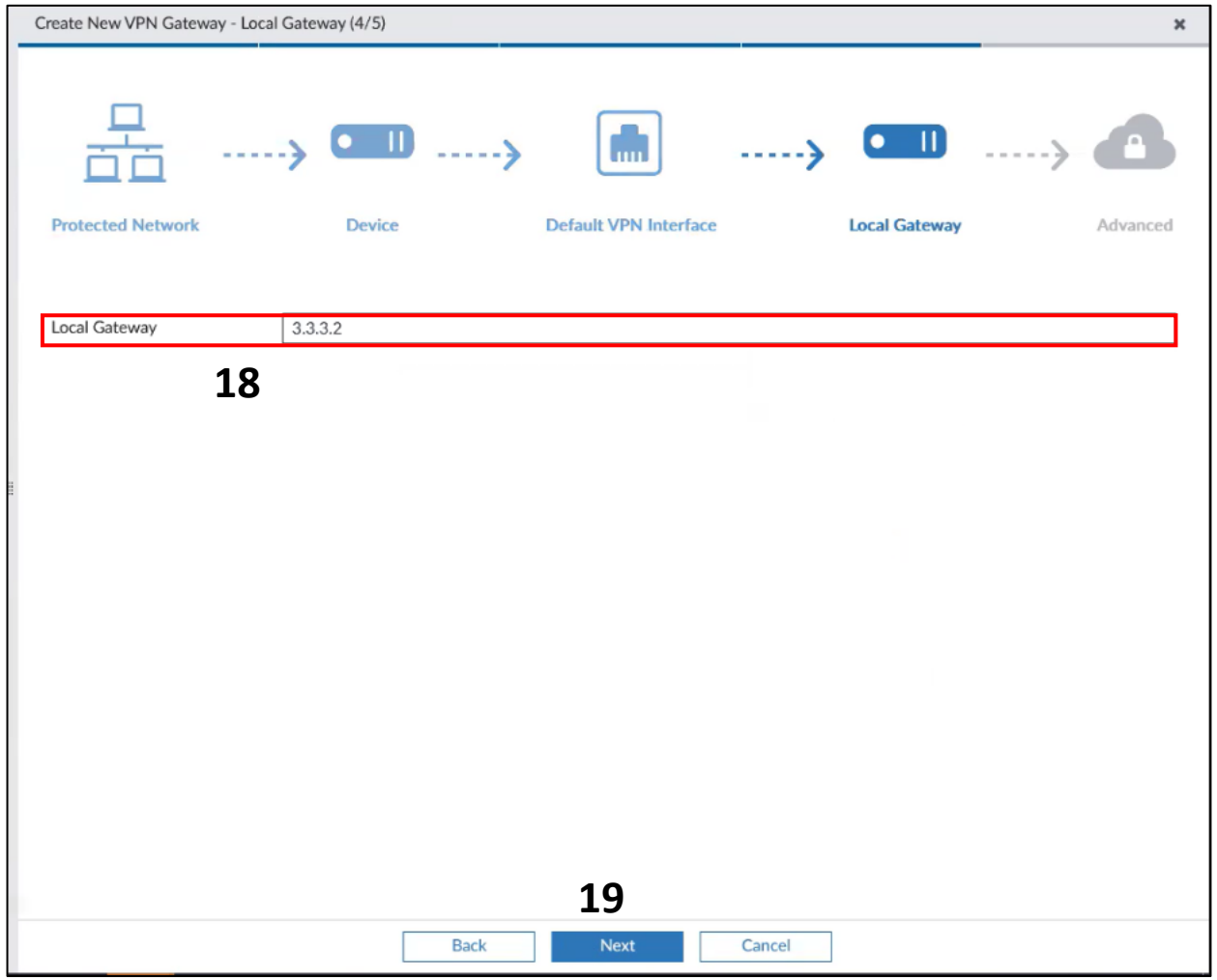
16. The "WAN" interface is selected, which is typically the interface connected to the internet.

17. Click the "Next" .

18. The IP address “3.3.3.2" is entered as the Local Gateway.

19. Click the "Next" .

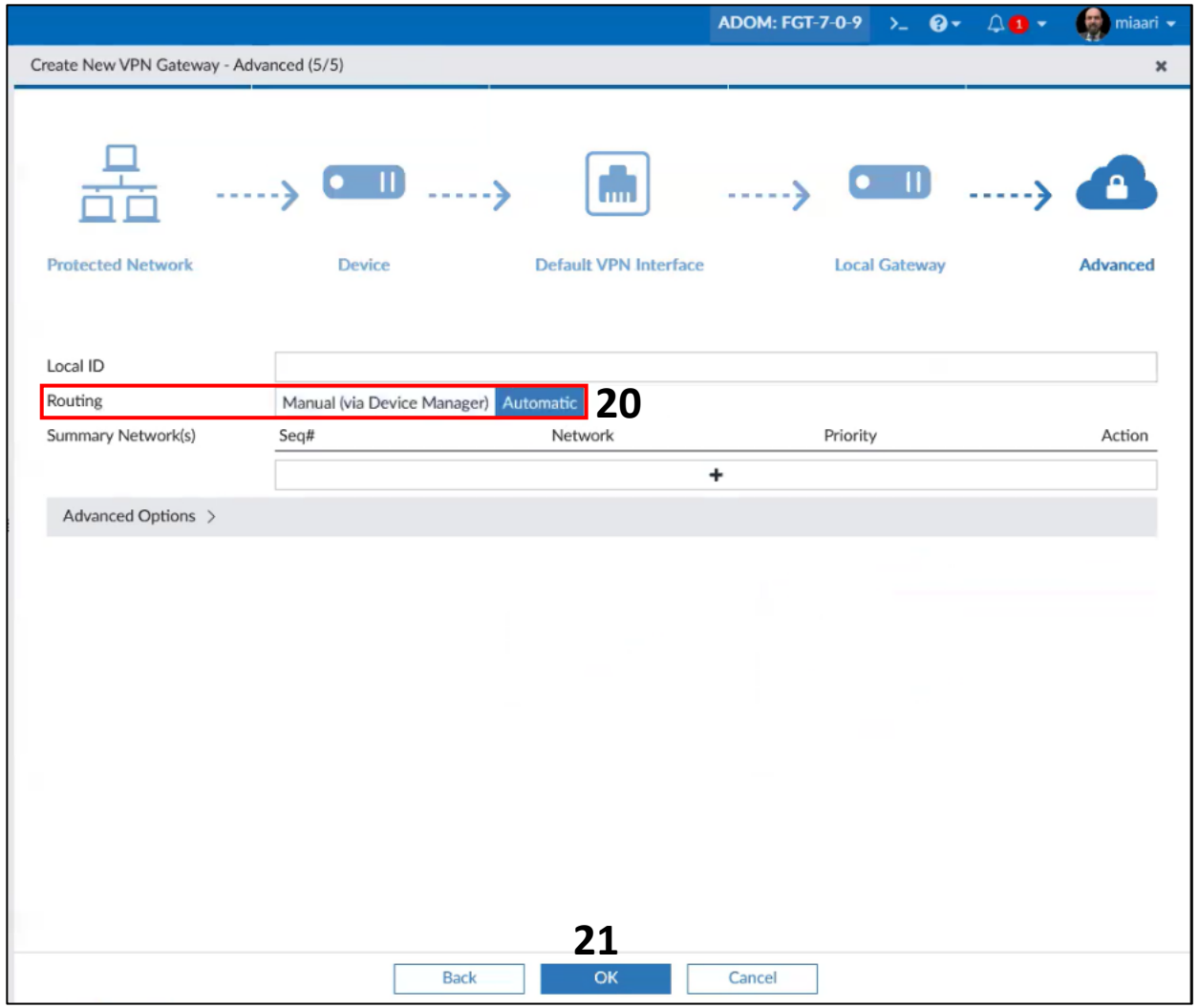


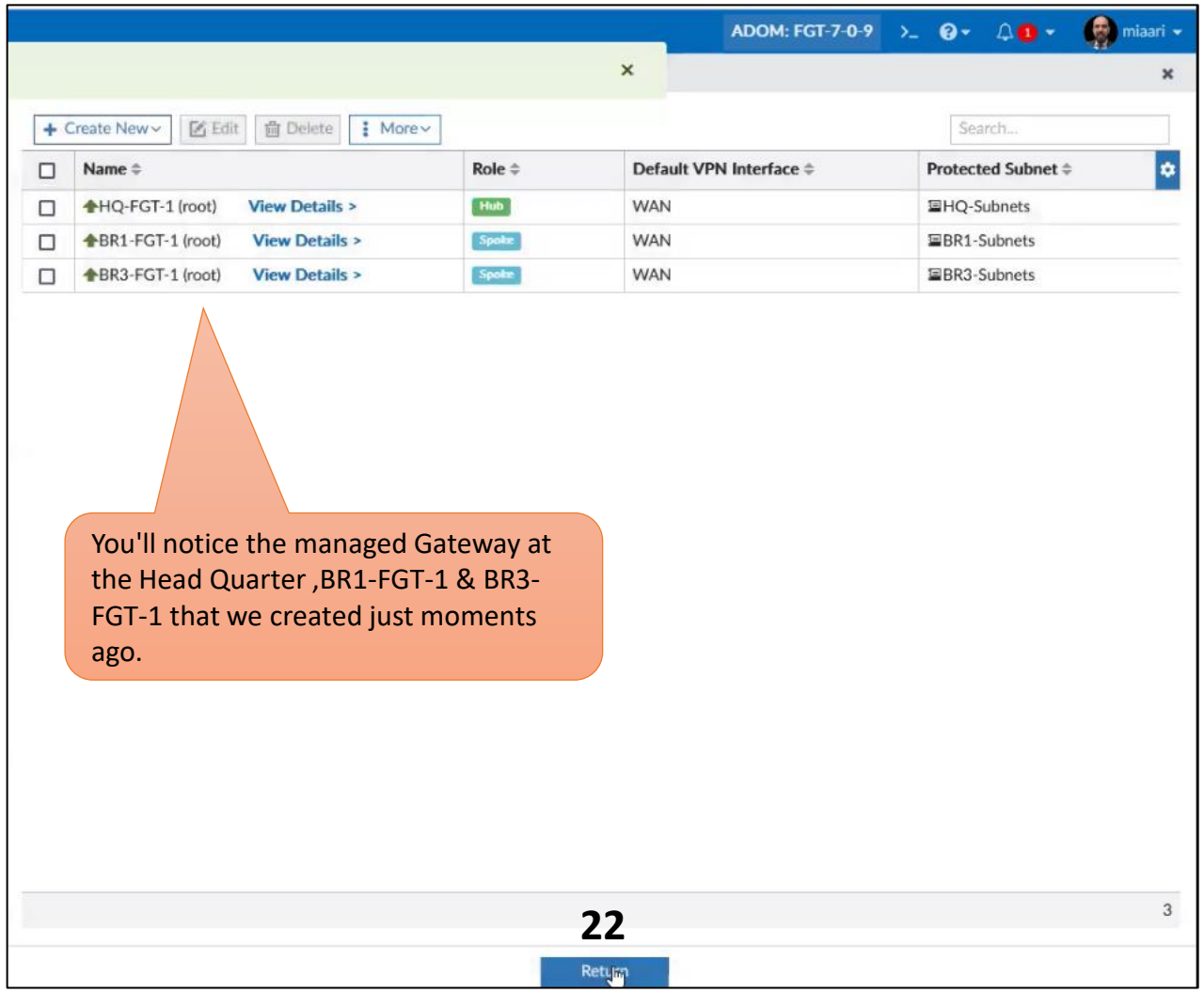


20. “Automatic” is selected.

21. Click the “OK” .

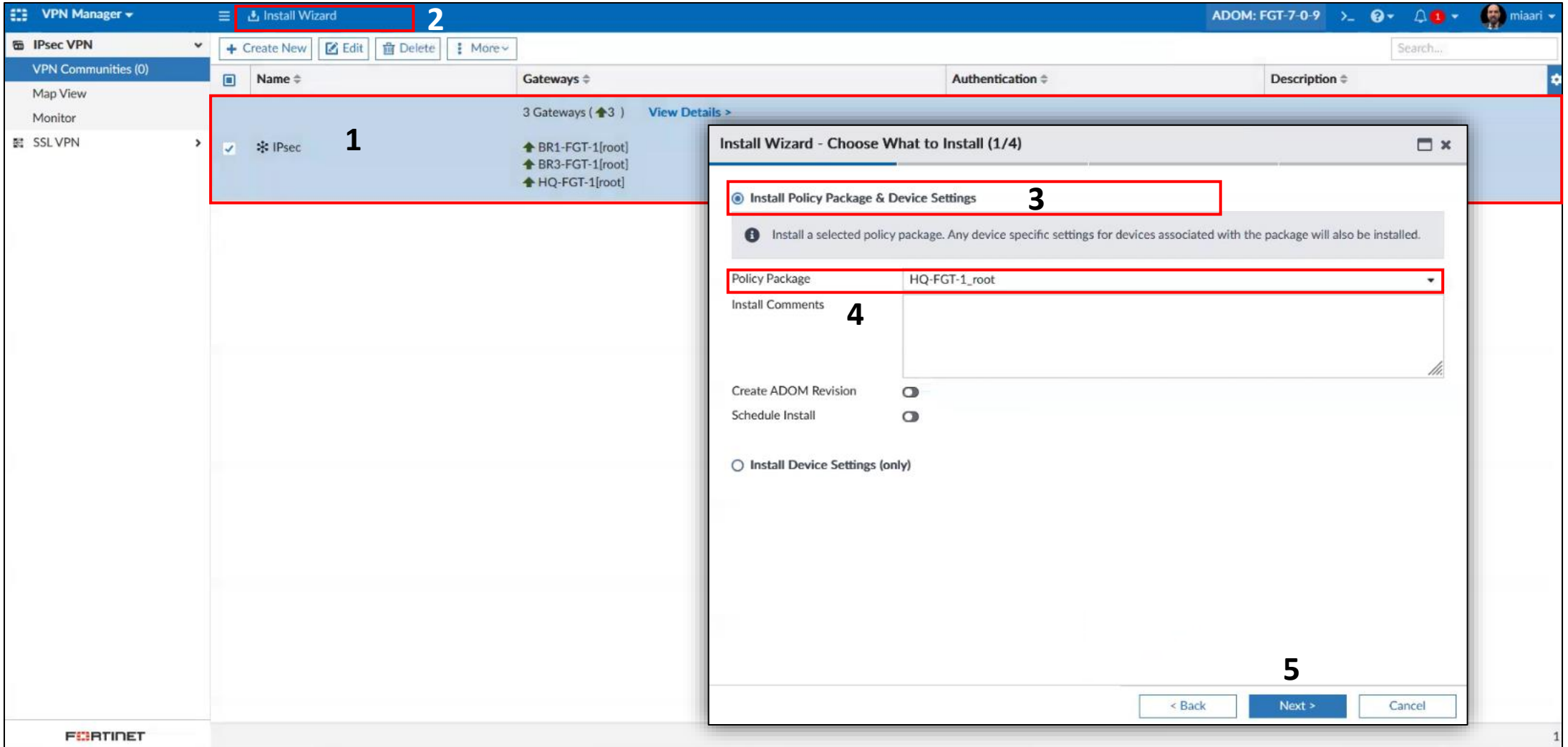
22. Click on “Return”.



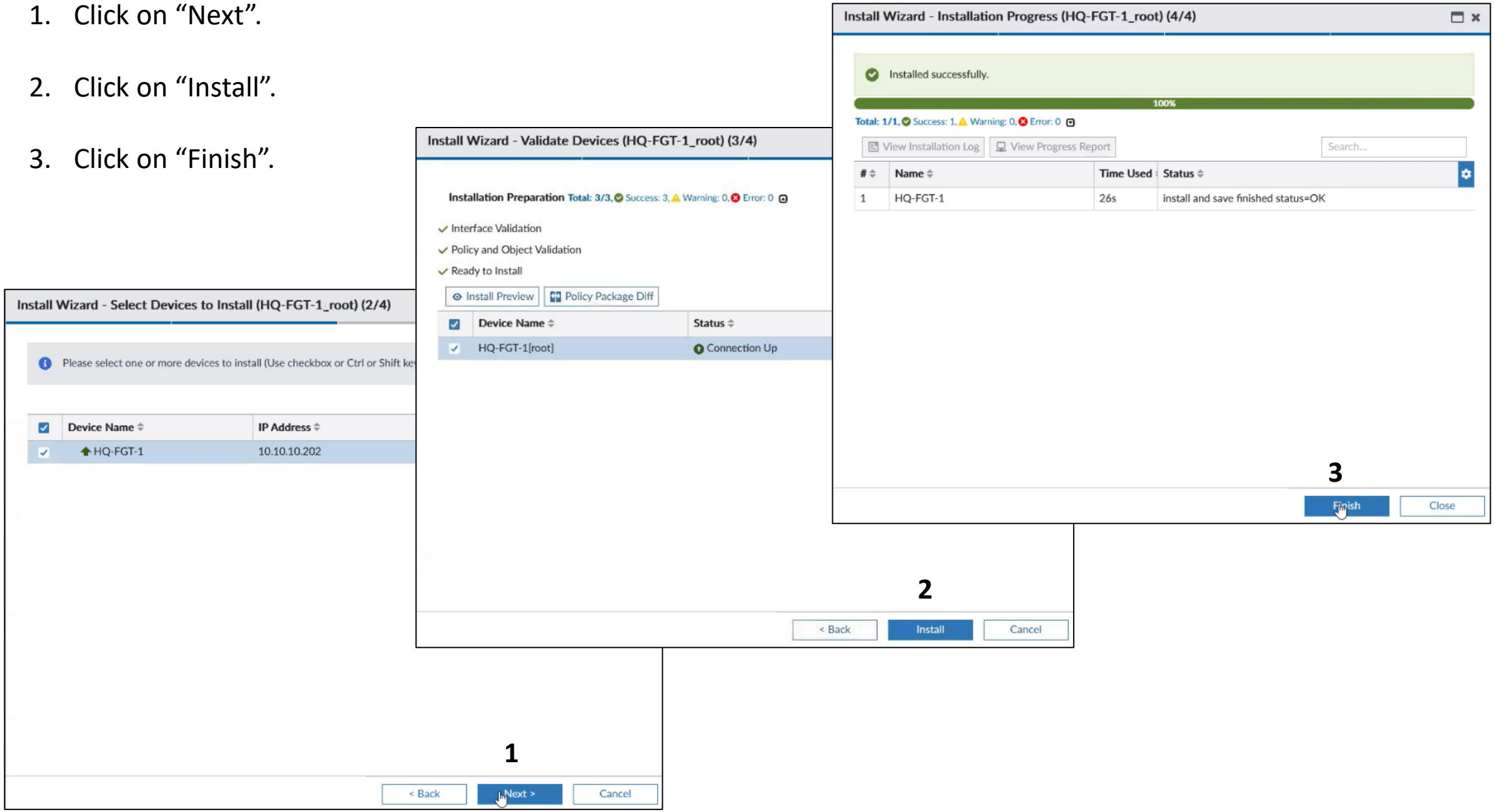


- To Install configuration on a FortiGate of Head Quarter :

1. Select the VPN Community you wish to configure by checking the box next to it , the "IPsec" VPN Community is selected.
2. Click on the "Install Wizard".
3. ensure that the option "Install Policy Package & Device Settings" is selected.
4. From the "Policy Package" dropdown menu, select "HQ-FGT-1_root" .
5. click the "Next" .

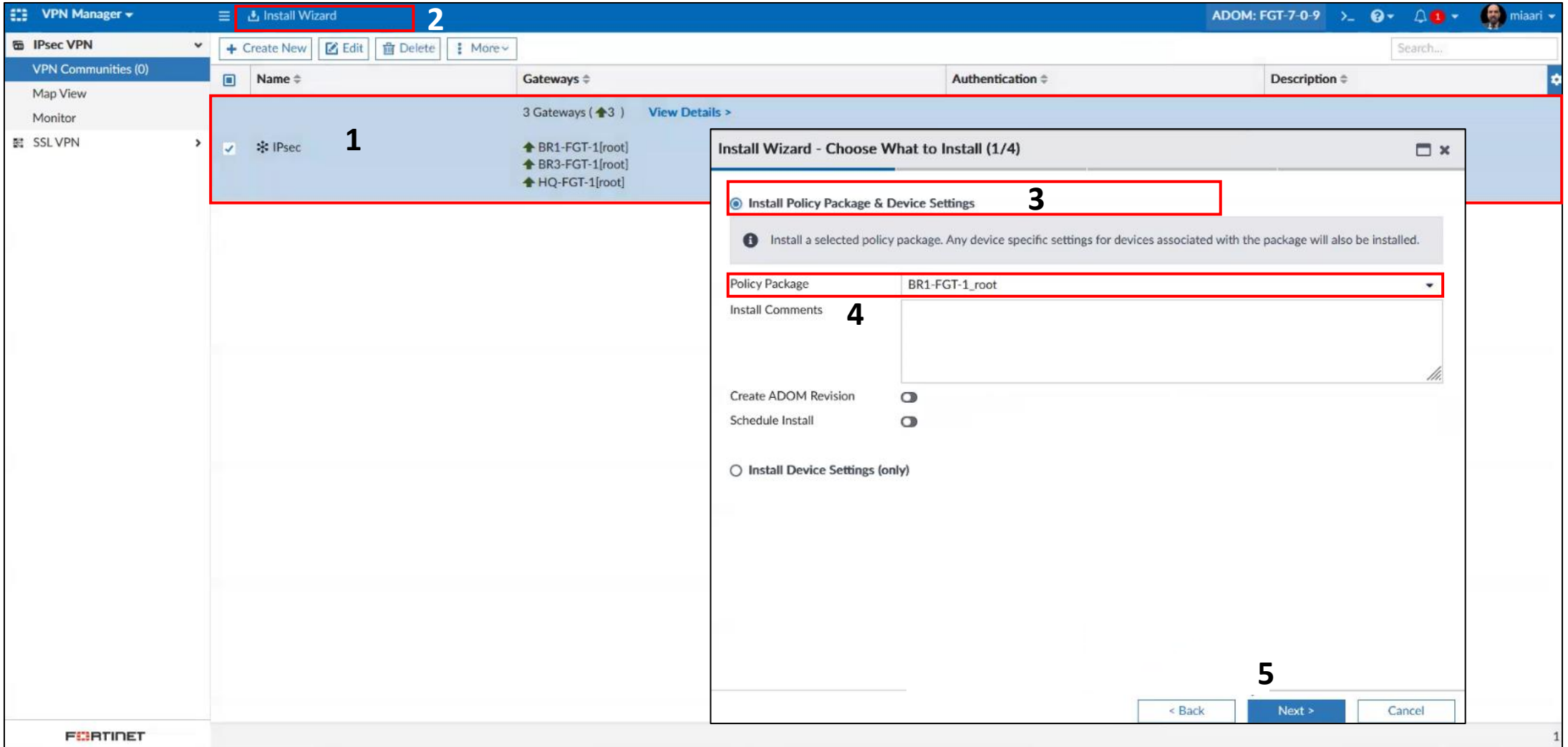


1. Click on “Next”.
2. Click on “Install”.
3. Click on “Finish”.

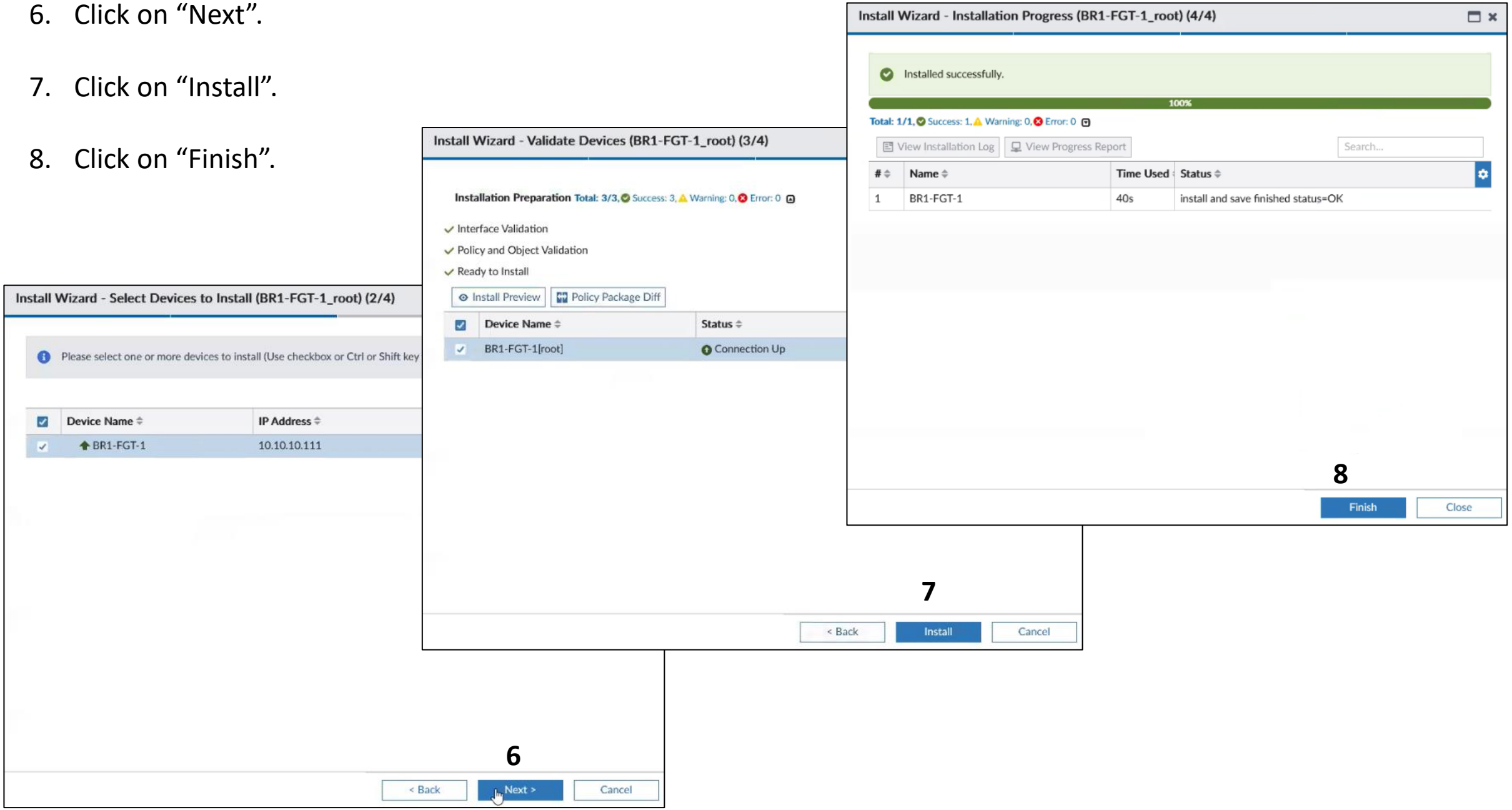


- **To Install configuration on a FortiGate of Branch-1:**

1. Select the VPN Community you wish to configure by checking the box next to it , the "IPsec" VPN Community is selected.
2. Click on the "Install Wizard".
3. ensure that the option "Install Policy Package & Device Settings" is selected.
4. From the "Policy Package" dropdown menu, select “BR1-FGT-1_root".
5. click the "Next" .

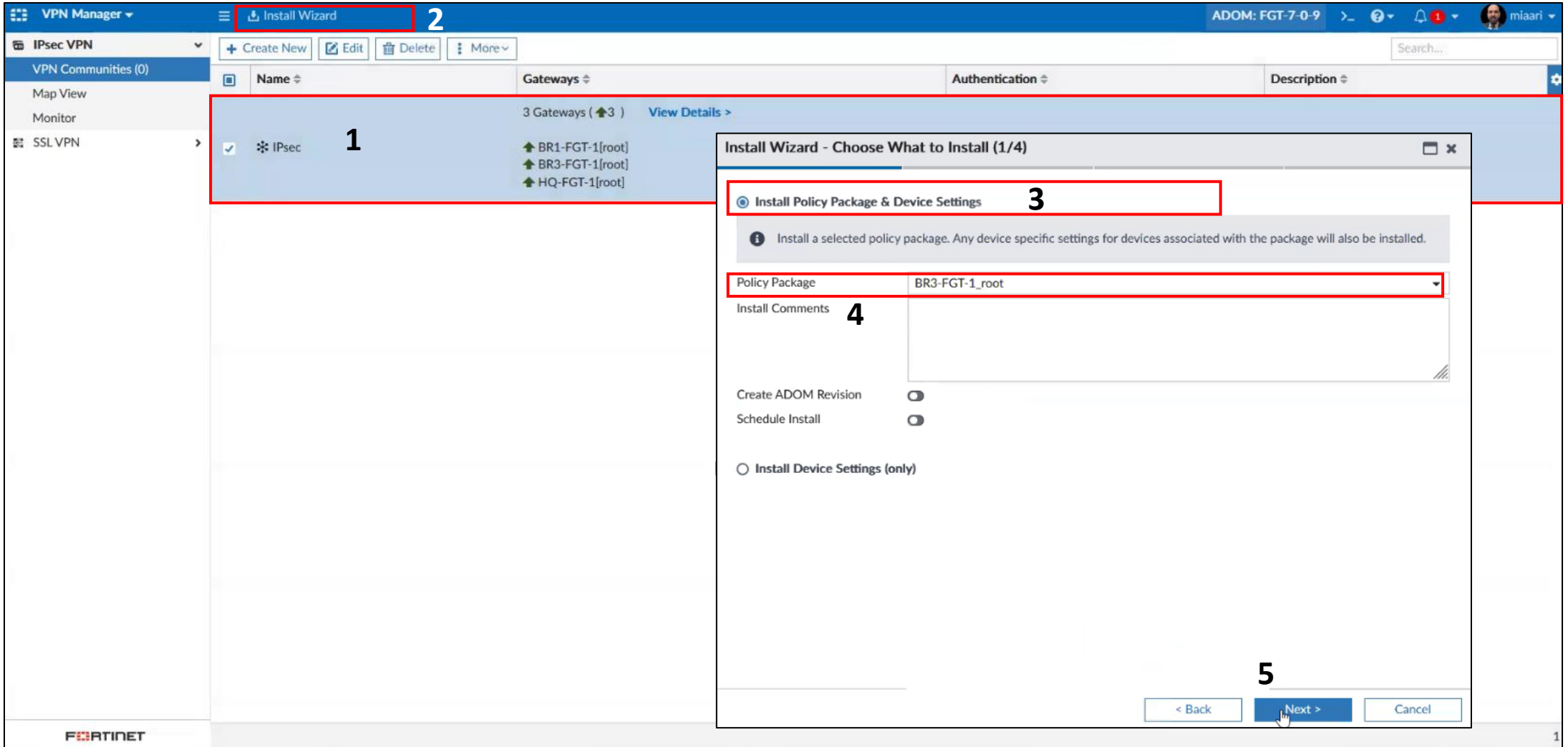


6. Click on “Next”.
7. Click on “Install”.
8. Click on “Finish”.

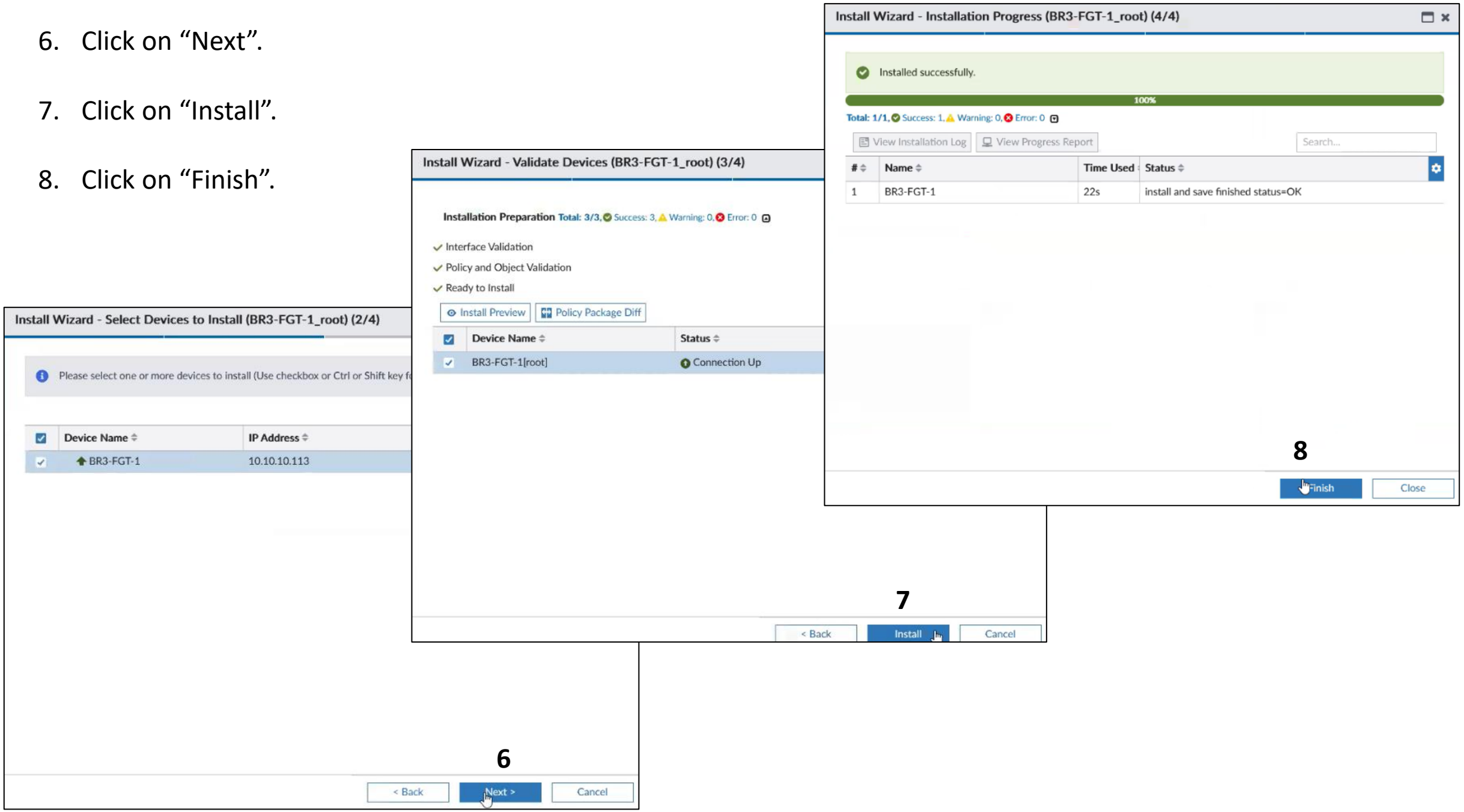


- **To Install configuration on a FortiGate of Branch-3:**

1. Select the VPN Community you wish to configure by checking the box next to it , the "IPsec" VPN Community is selected.
2. Click on the "Install Wizard".
3. ensure that the option "Install Policy Package & Device Settings" is selected.
4. From the "Policy Package" dropdown menu, select “BR3-FGT-1_root" .
5. click the "Next" .



6. Click on “Next”.
7. Click on “Install”.
8. Click on “Finish”.



- To confirm that the devices have successfully pulled the configuration:

➢ Accessing the FortiGate using the GUI

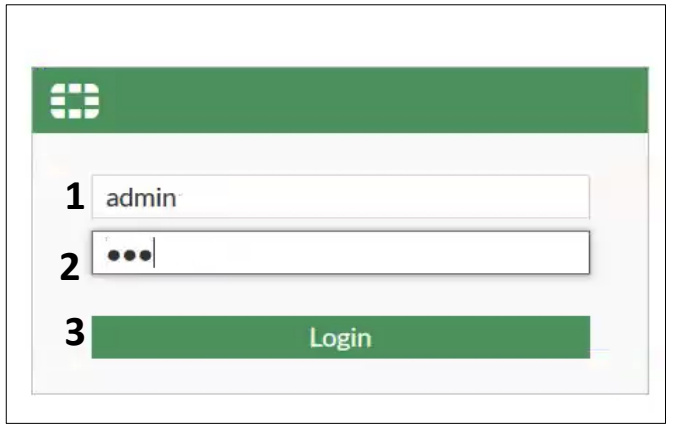
Open your browser and:

1. use the Management IP Address for the HQ-FGT-1 in Head Quarter (10.10.10.202).
2. use the Management IP Address for the BR1-FGT-1 in Branch-1 (10.10.10.111).
3. use the Management IP Address for the BR3-FGT-1 in Branch-3 (10.10.10.113).

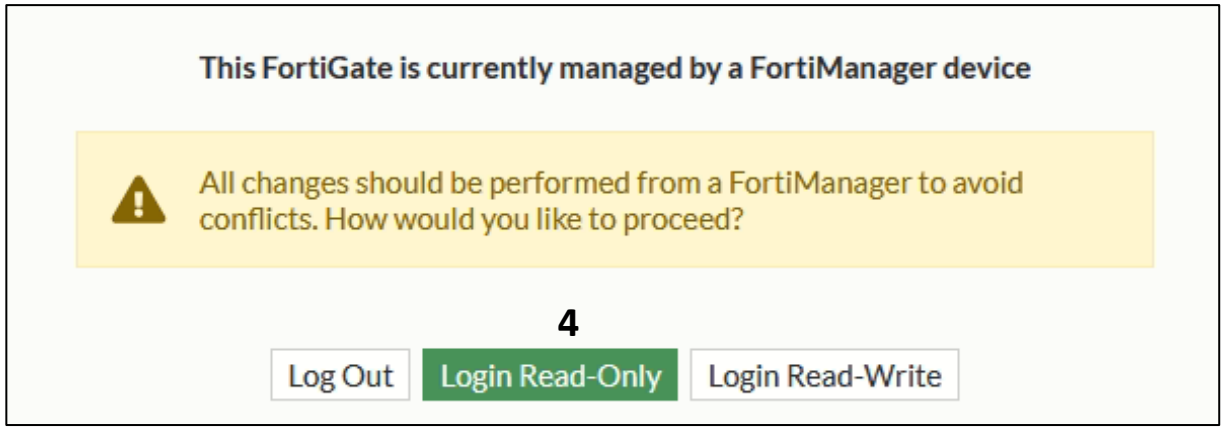
1.Enter Username (admin)

2.Enter Password (123)

3.Login



4.Click on “Login Read-Only”.



HQ-FGT-1

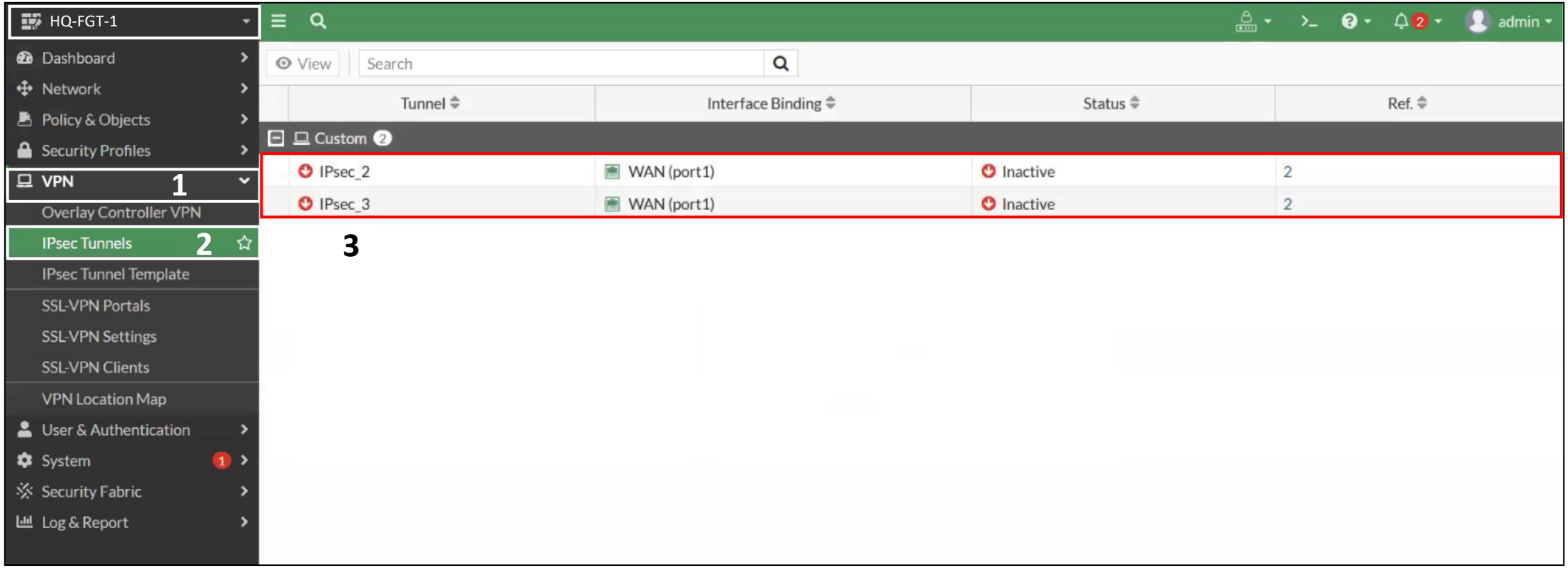
1. On the left-hand side of the FortiGate interface, navigate to the "VPN" section

2. Under the "VPN" menu, click on "IPsec Tunnels." This will display the list of all IPsec tunnels configured on the FortiGate device.

3. The main window will show a list of IPsec tunnels, two tunnels are displayed:

- **IPsec_2:** Bound to the WAN interface (port1), which is intended for Branch-1 .
- **IPsec_3:** Also bound to the WAN interface (port1), which is intended for Branch-3 .

Both tunnels show a status of "Inactive," indicating that the tunnels are currently not active or established.



BR1-FGT-1

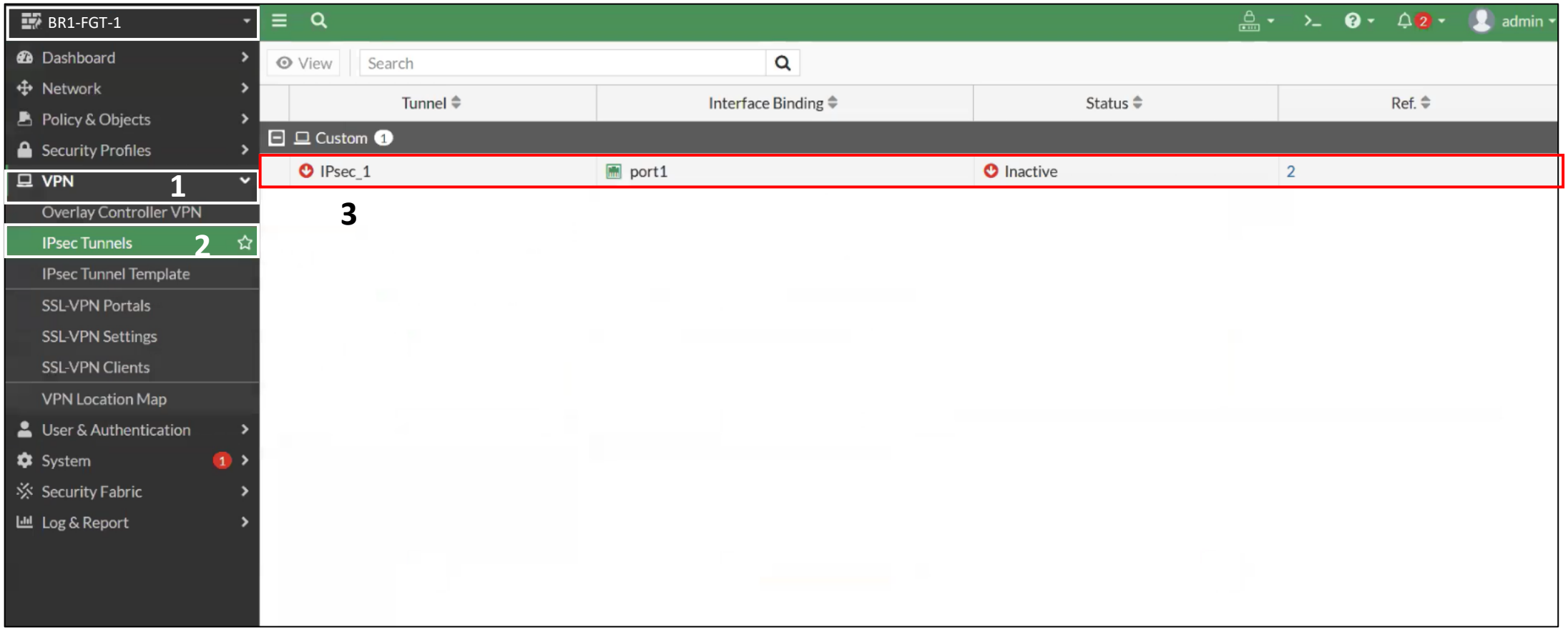
1. On the left-hand side of the FortiGate interface, navigate to the "VPN" section

2. Under the "VPN" menu, click on "IPsec Tunnels." This will display the list of all IPsec tunnels configured on the FortiGate device.

3. The main window will show a list of IPsec tunnels, two tunnels are displayed:

- **IPsec_1:** Bound to the WAN interface (port1), which is intended for HQ-FGT-1

Both tunnels show a status of "Inactive," indicating that the tunnels are currently not active or established.



BR3-FGT-1

1. On the left-hand side of the FortiGate interface, navigate to the "VPN" section

2. Under the "VPN" menu, click on "IPsec Tunnels." This will display the list of all IPsec tunnels configured on the FortiGate device.

3. The main window will show a list of IPsec tunnels, two tunnels are displayed:

- **IPsec_1:** Bound to the WAN interface (port1), which is intended for HQ-FGT-1

Both tunnels show a status of "Inactive," indicating that the tunnels are currently not active or established.