10.5 Deploy FortiGate in AWS

Learning Objectives

- Create a VPC, public and private subnet, internet gateway, route tables
- Create a FortiGate firewall in AWS through Marketplace
- Identify FortiGate subnets in AWS

Scenario: In this lab, we'll learn how to deploy FortiGate in AWS.

AWS Configuration

1. Create a VPC.

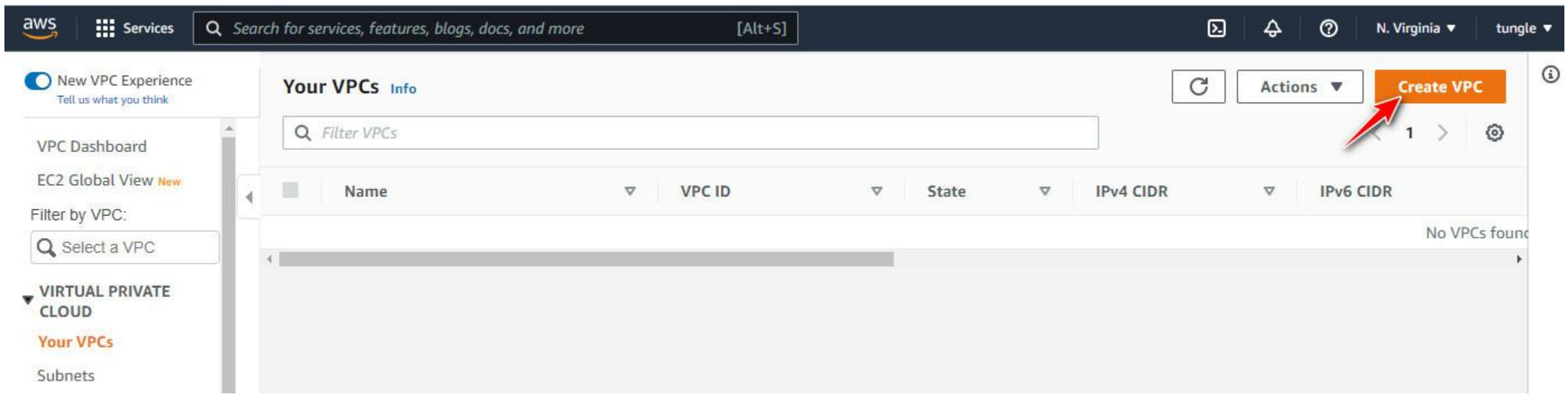

Figure 10.107: Create a VPC

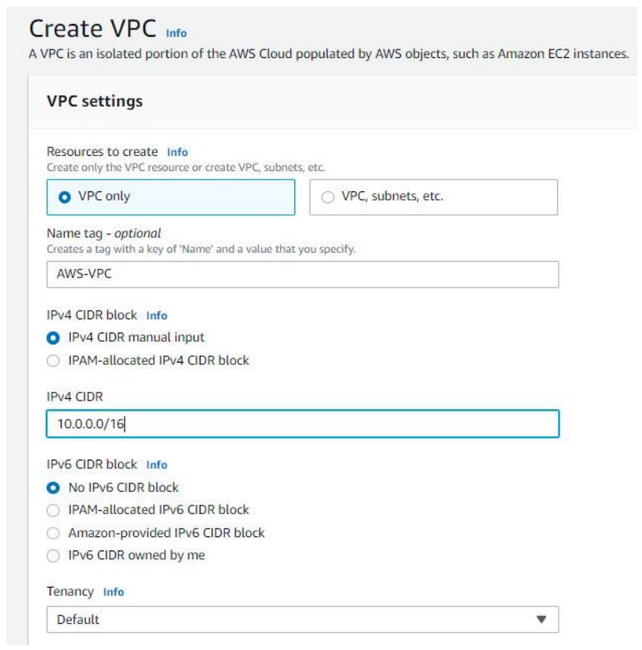

Figure 10.108: Create a VPC named "AWS-VPC"

2. Create a subnet.

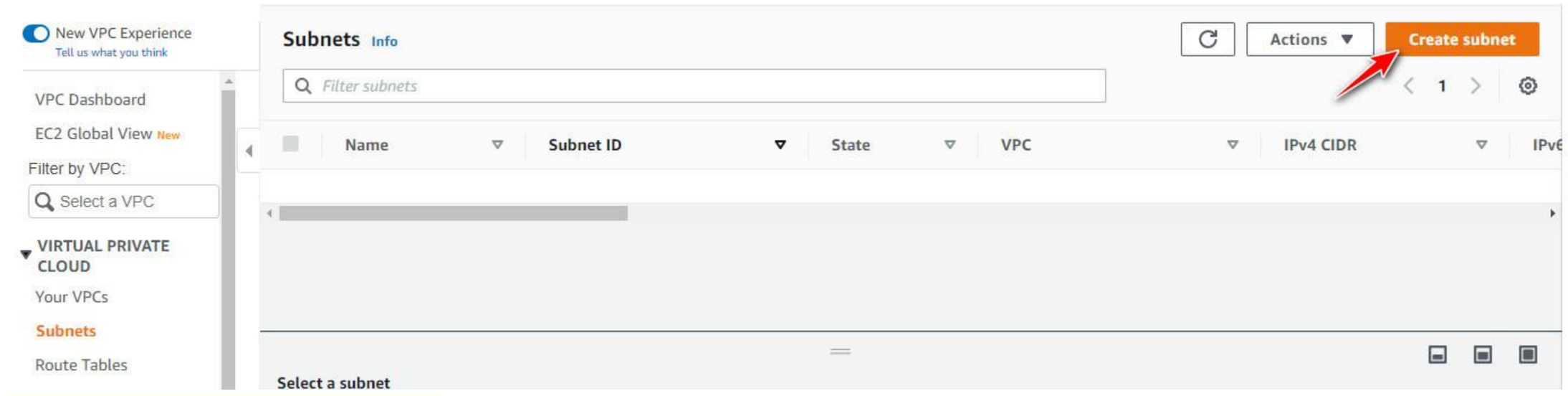

Figure 10.109: Create a subnet

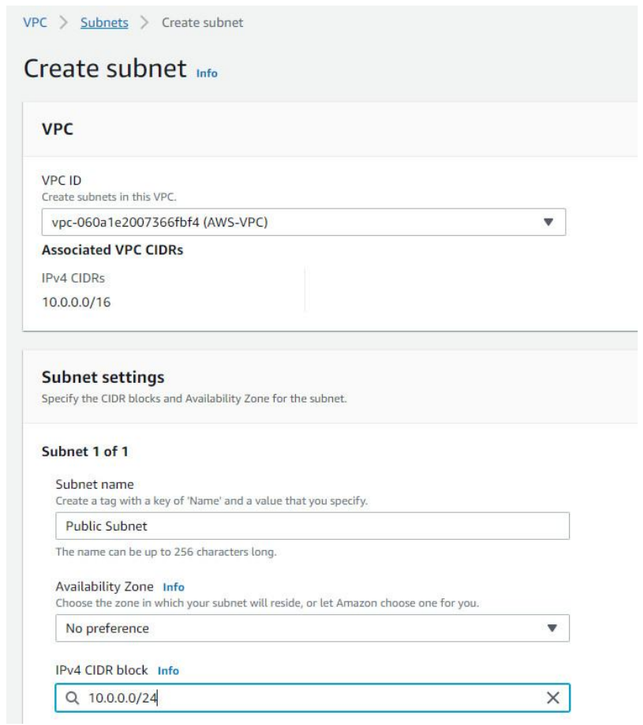

Figure 10.110: Create a public subnet under AWS-VPC

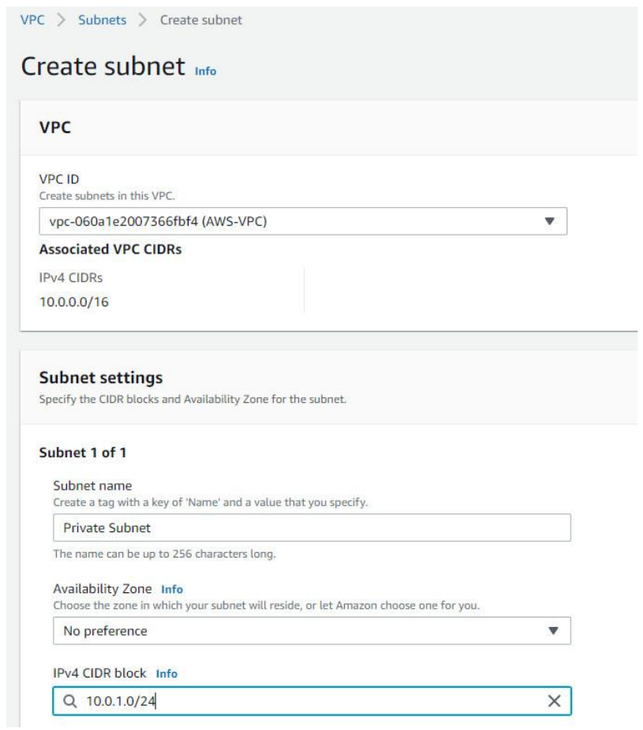

Figure 10.111: Create an internet gateway under AWS-VPC

3. Create an internet gateway.

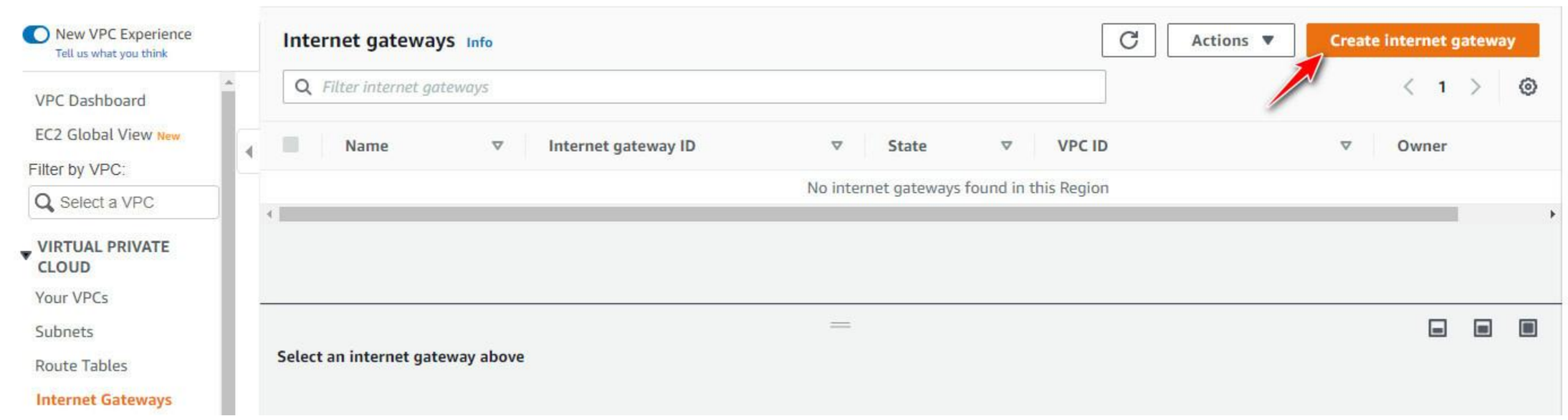

Figure 10.112: Create an internet gateway

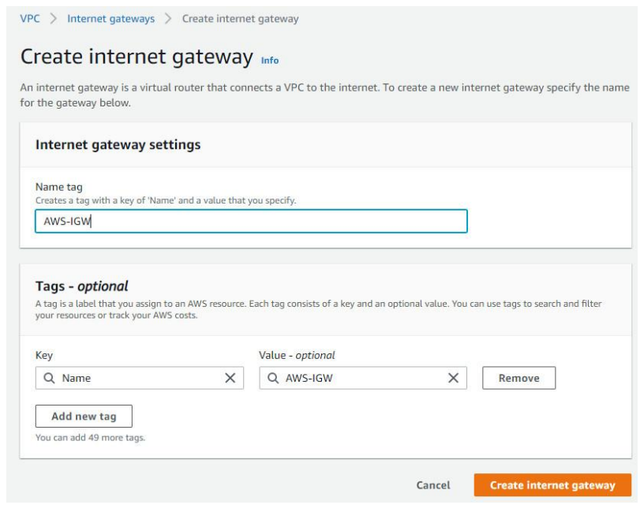

Figure 10.113: Create an internet gateway

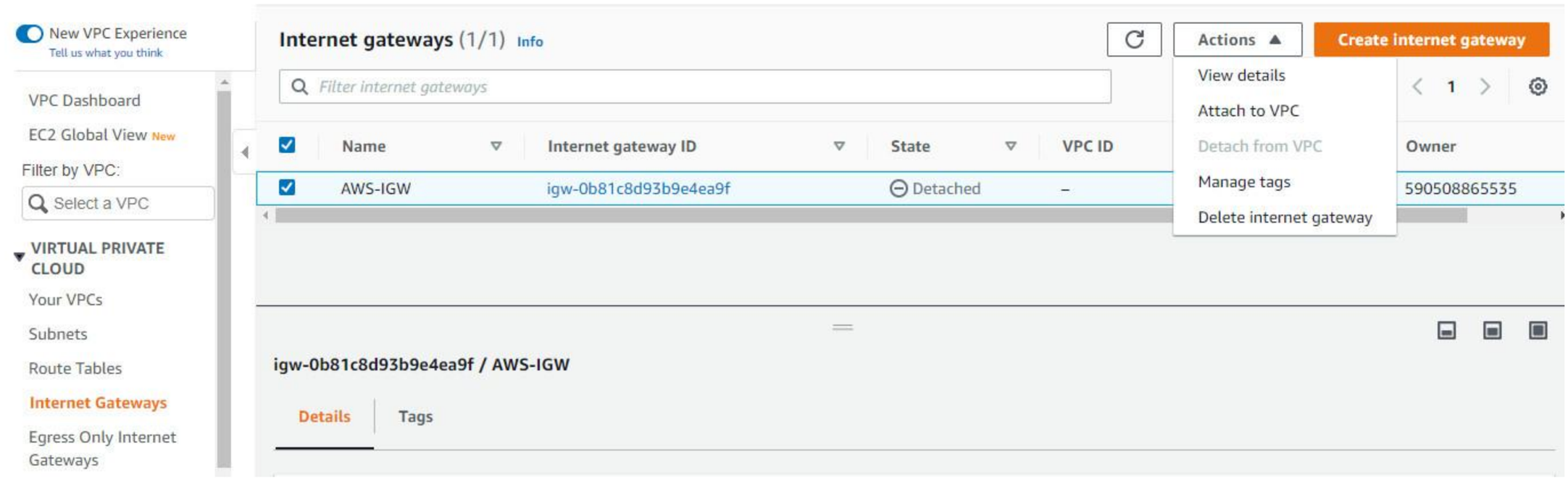

Figure 10.114: Attach an internet gateway to VPC

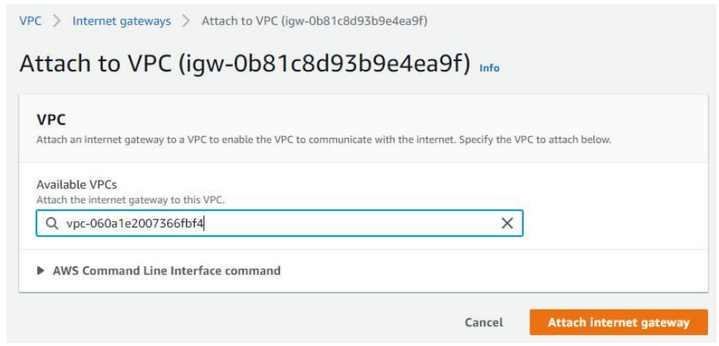

Figure 10.115: Attach an internet gateway to VPC

4. Create a new Public RouteBy default, name of the “built-in route” is “-”. Rename it to Private Route.

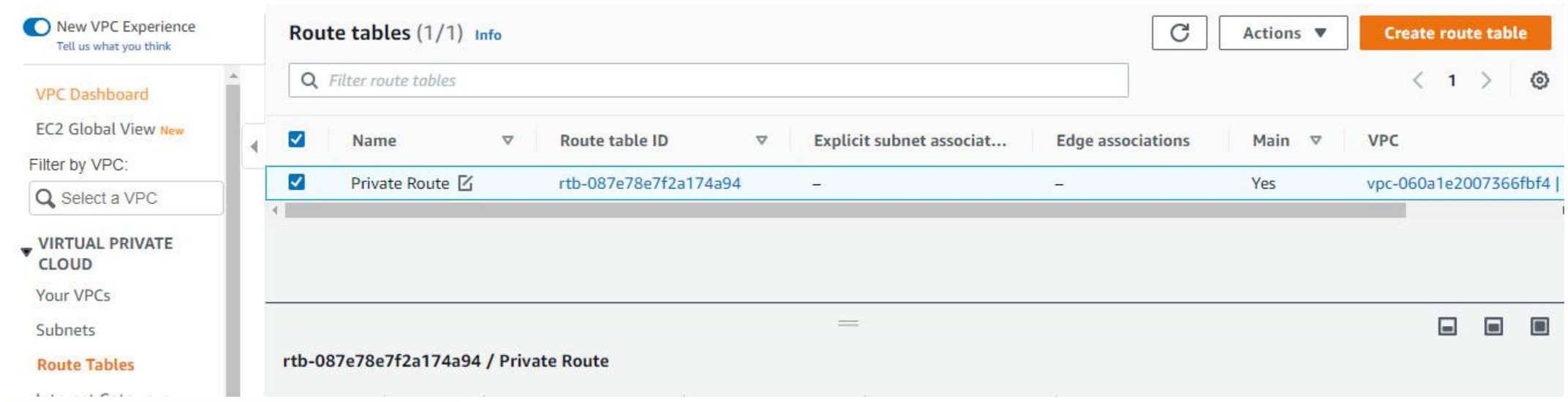

Figure 10.116: Edit private route

Go to **Route tables** > **create route table**.

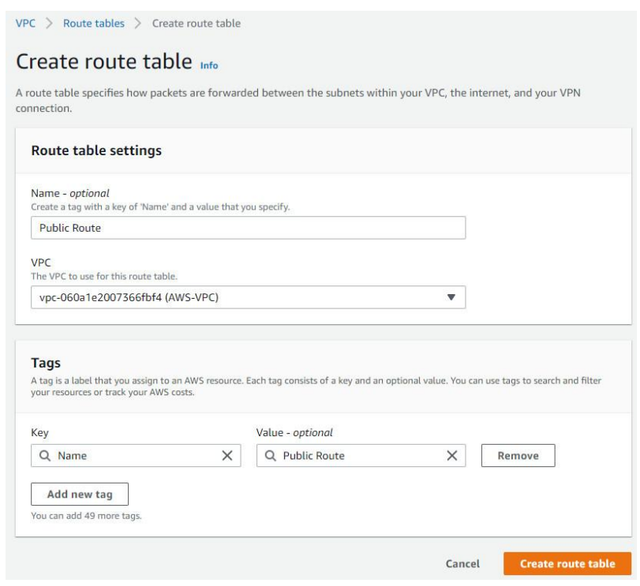

Figure 10.117: Create a public route

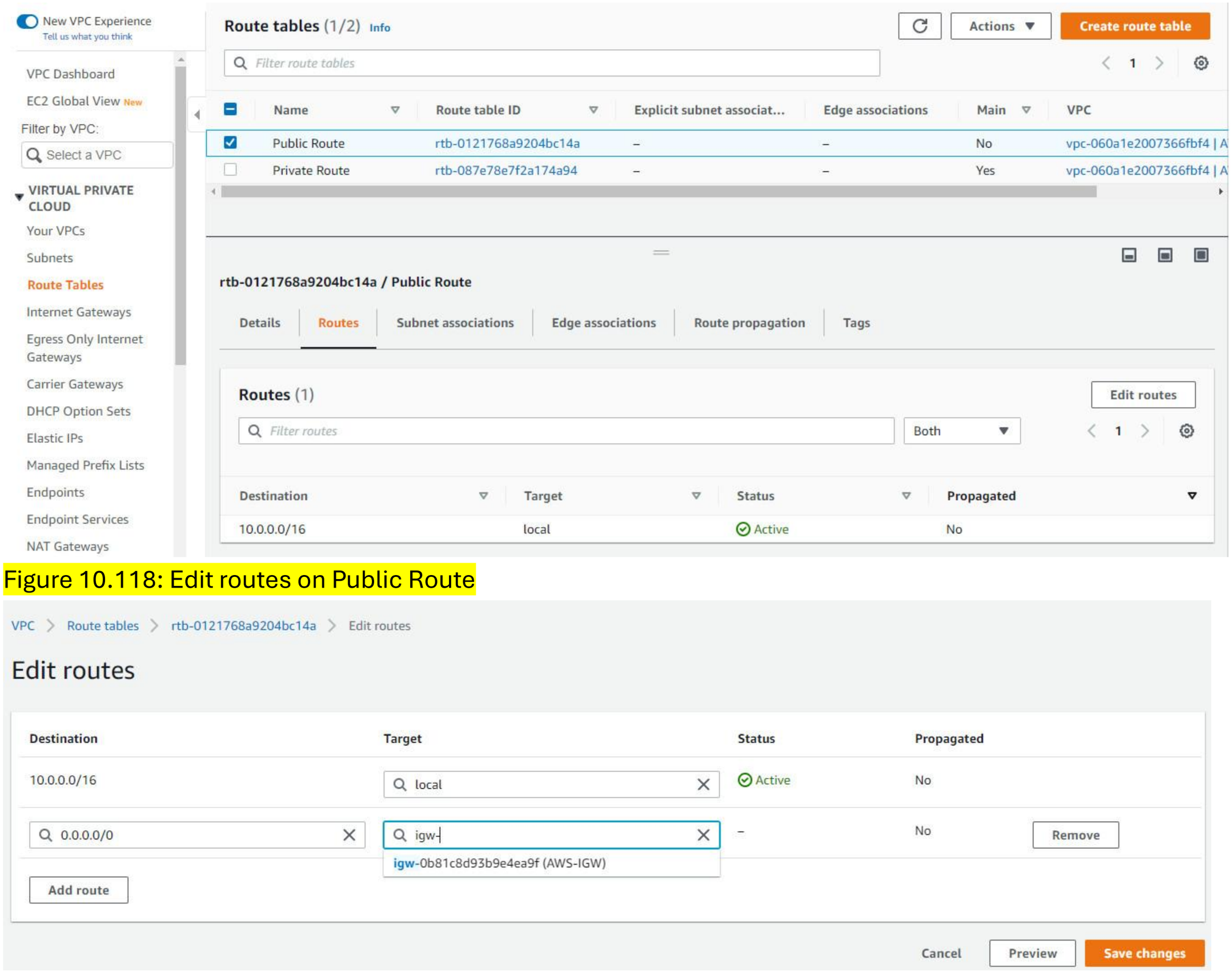

Figure 10.118: Edit routes on Public Route

Figure 10.119: Create a new default route to the internet gateway

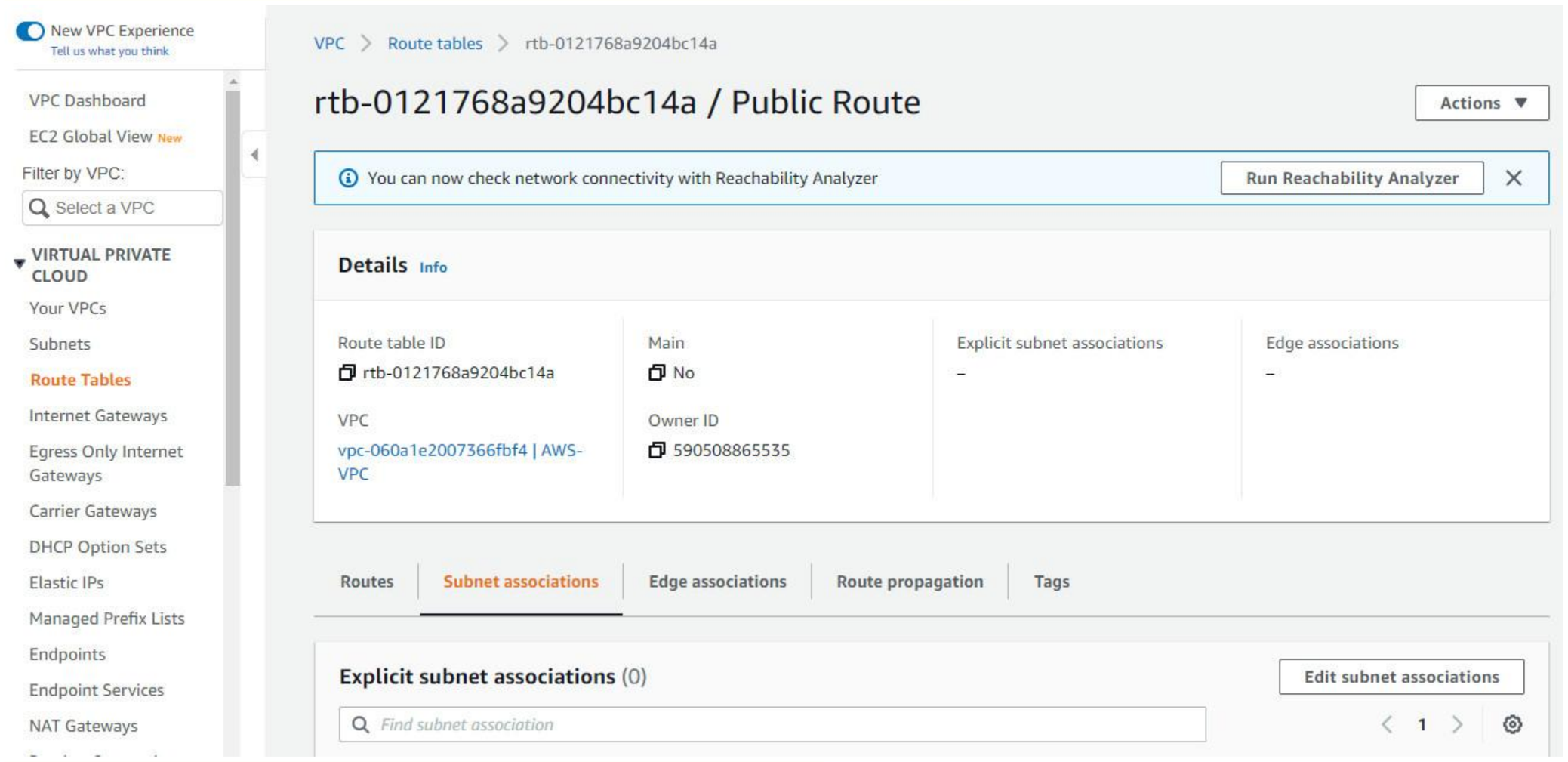

Figure 10.120: Associate Public Subnet to Public Route

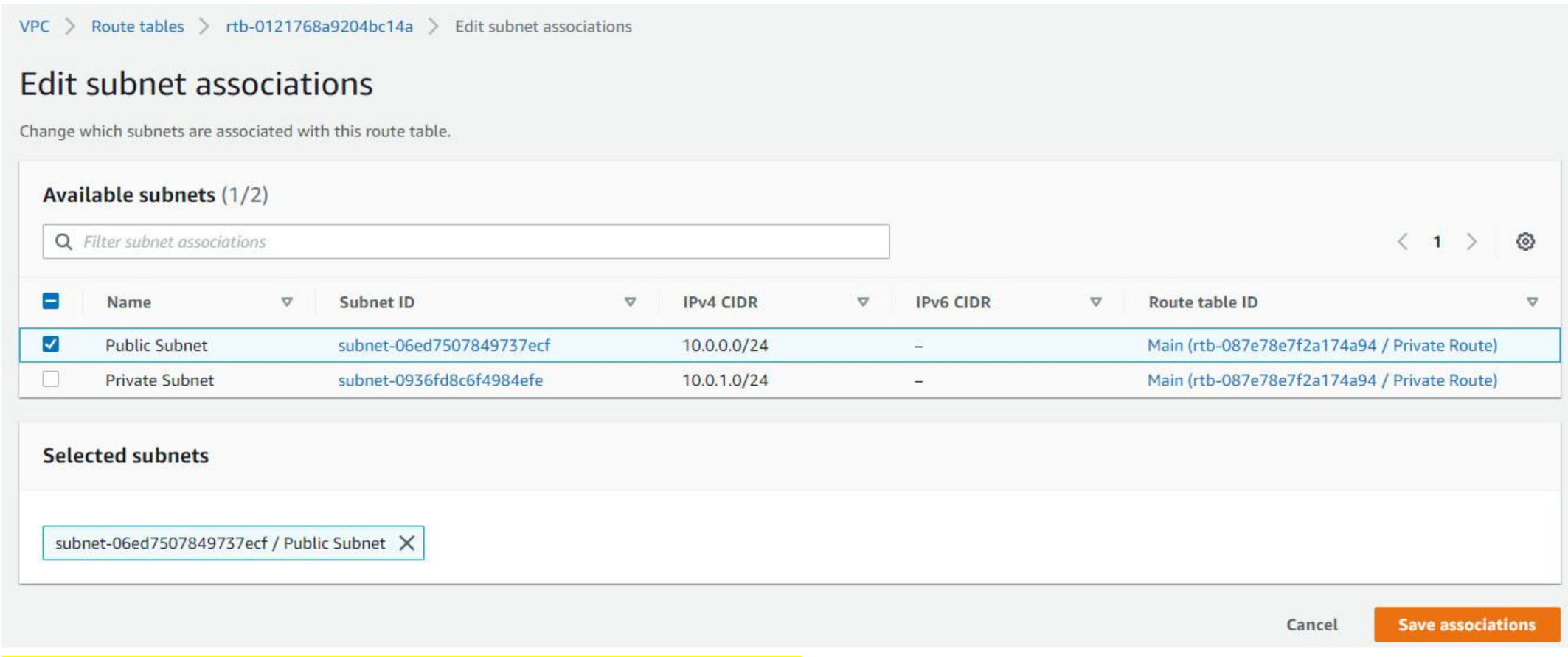

Figure 10.121: Associate Public Subnet to Public Route

5. Create Key Pair. Go to **EC2 – Key Pairs > Create Key Pair**.

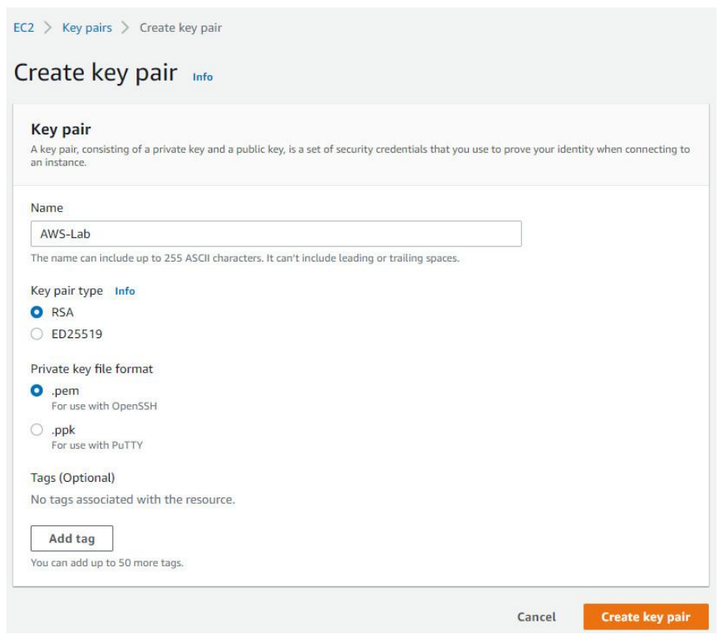

Figure 10.122: Create a key pair

6. Create Instances. Go to **EC2 – Instances** > **Launch instances**.

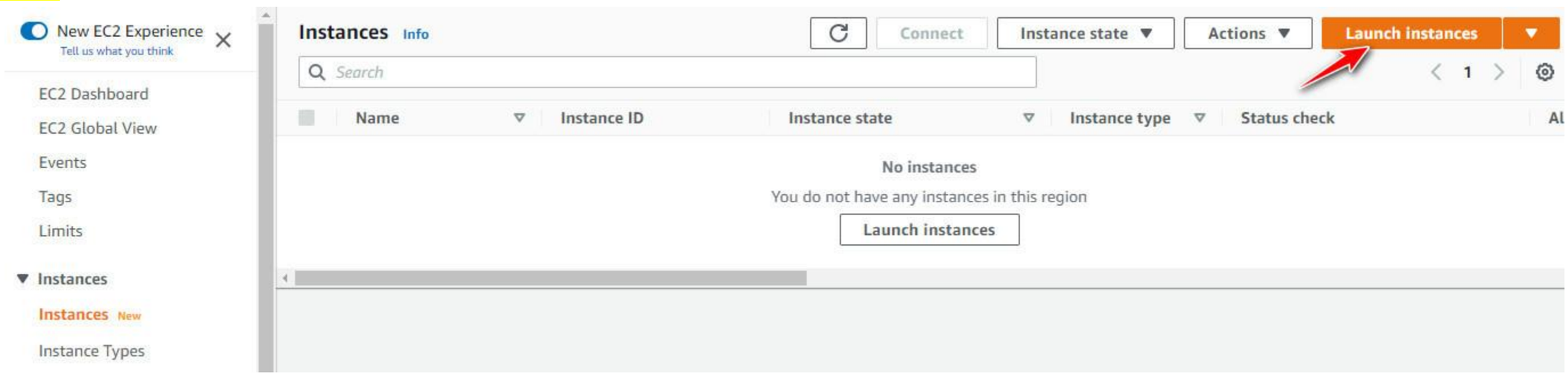

Figure 10.123: Launch a FortiGate instance

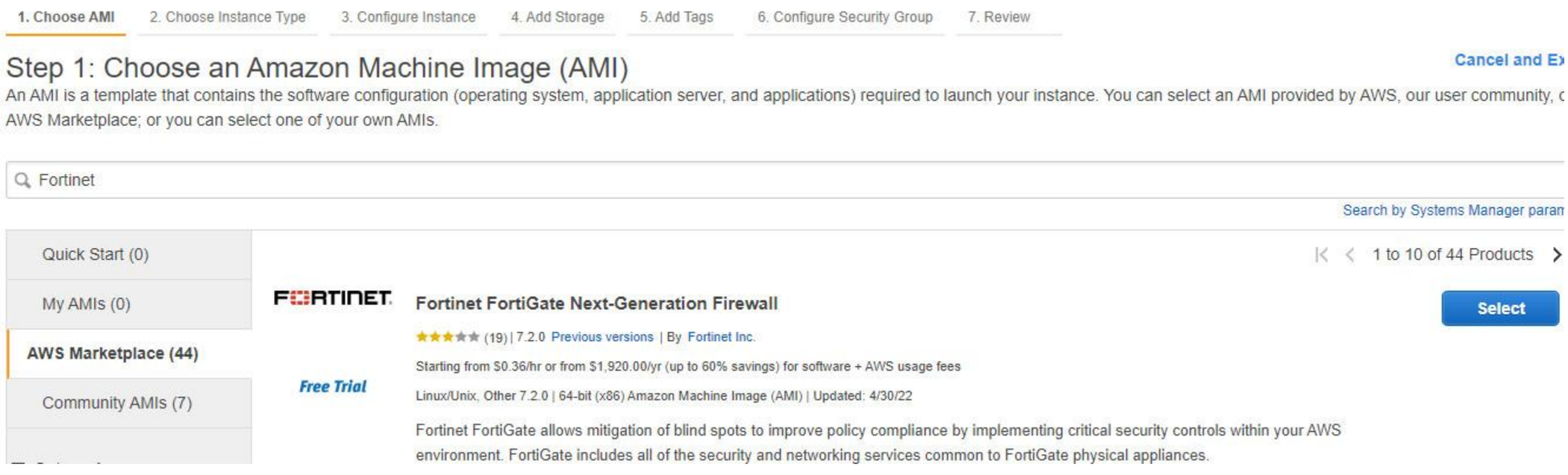

Figure 10.124: Select Fortinet FortiGate Next-Generation Firewall

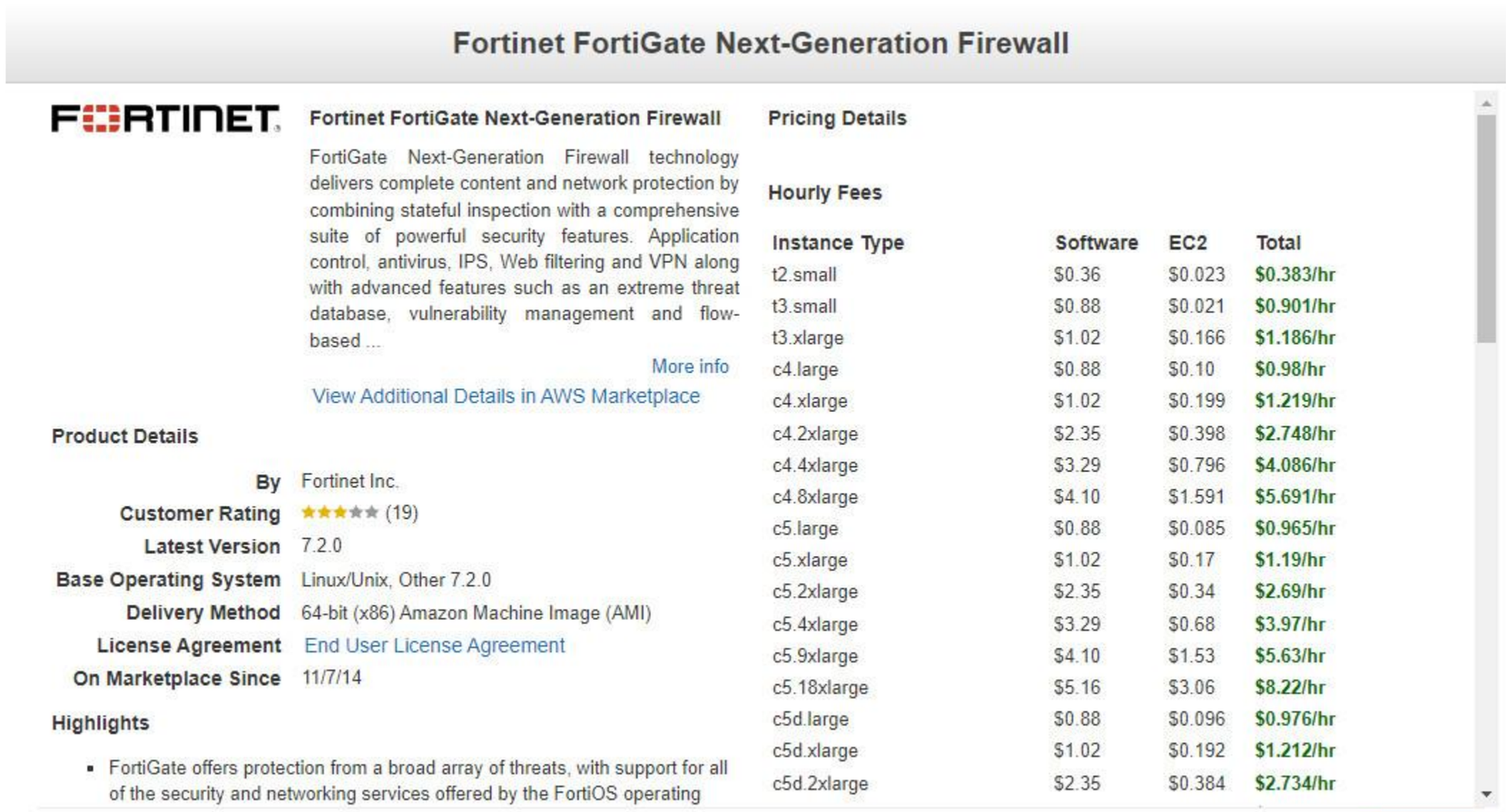

Figure 10.125: Accept FortiGate licence

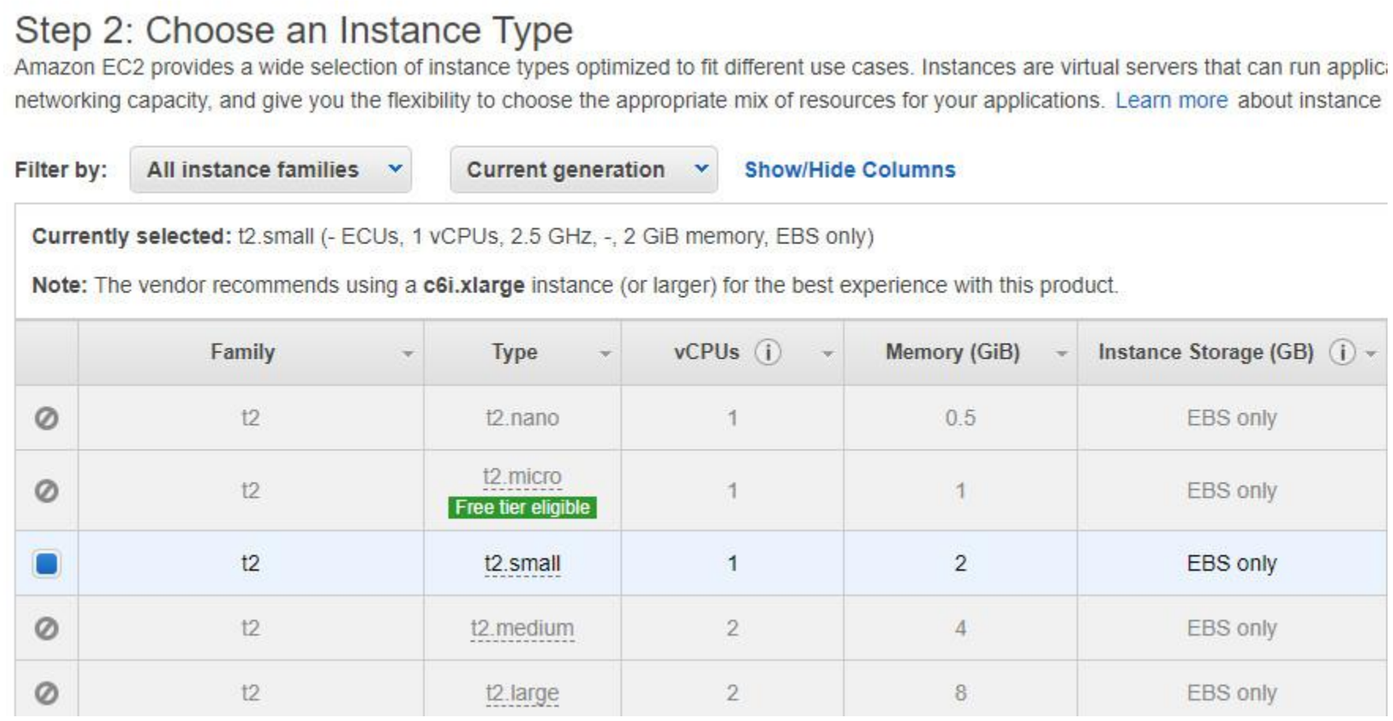

Figure 10.126: Select FortiGate instance type

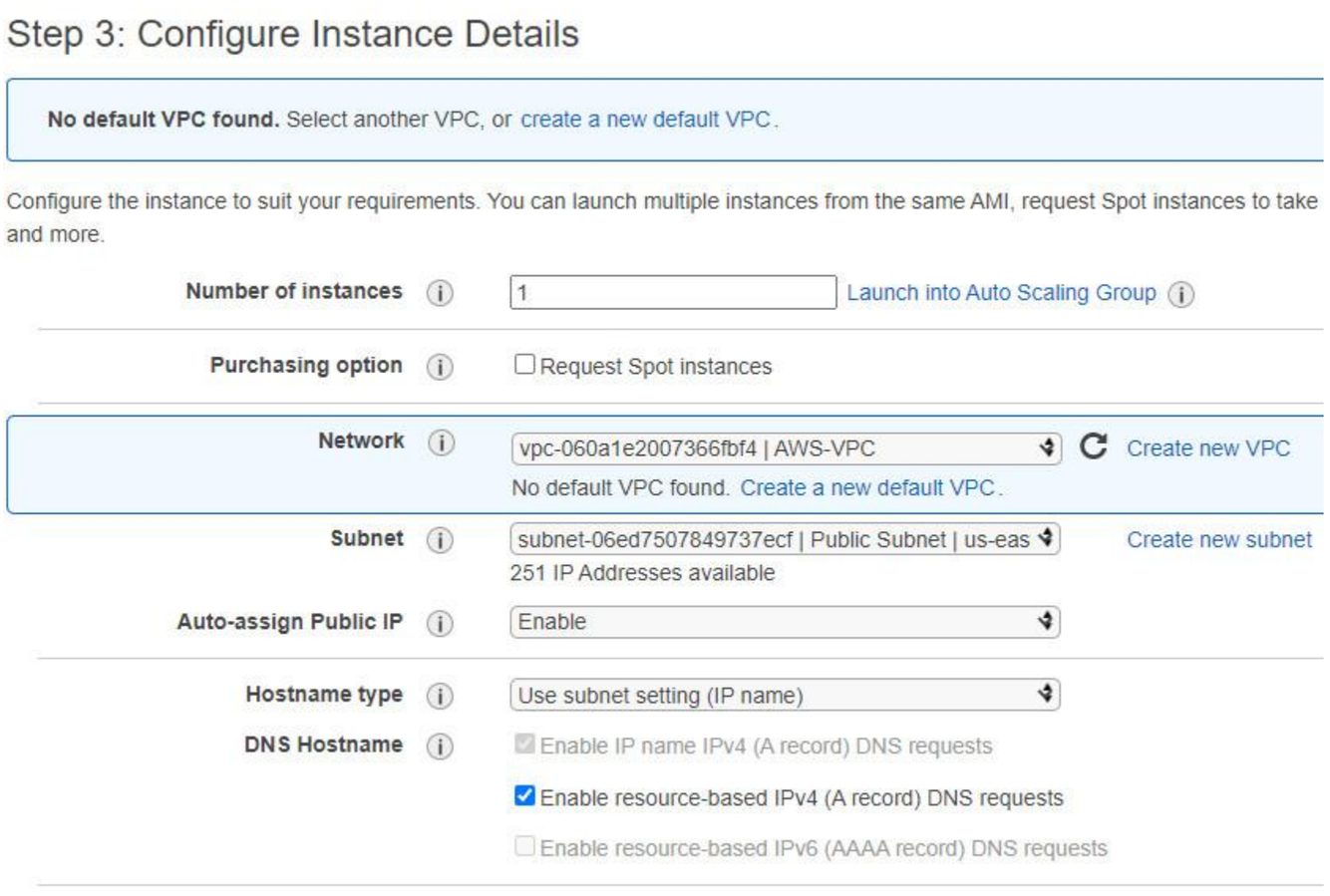

Figure 10.127: Select Network is “AWS-VPC”, Subnet is “Public Subnet” and Auto-assign Public IP is “Enable”

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)
Root	/dev/sda1	snap-0ba9f2da5ecf96965	2	General Purpose SSD (gp2)	100 / 3000	N/A
EBS	/dev/sdb	Search (case-insensit	30	General Purpose SSD (gp2)	100 / 3000	N/A

Add New Volume

Figure 10.128: Leave the Add storage as the default

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances
Name	FG	☑

Figure 10.129: Assign Tag with Key is Name and Value is FG

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, i
Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing
security groups.

Assign a security group: ◉ Create a **new** security group
○ Select an **existing** security group

Security group name: FortiGate Security Group

Description: FortiGate Security Group

Type	Protocol	Port Range	Source	
SSH	TCP	22	Custom	0.0.0.0/0
HTTP	TCP	80	Custom	0.0.0.0/0
HTTPS	TCP	443	Custom	0.0.0.0/0
Custom TCP F	TCP	541	Custom	0.0.0.0/0
Custom TCP F	TCP	3000	Custom	0.0.0.0/0
Custom TCP F	TCP	8080	Custom	0.0.0.0/0
RDP	TCP	3389	Custom	0.0.0.0/0
All ICMP - IPv	ICMP	0 - 65535	Custom	0.0.0.0/0

Add Rule

Figure 10.130: Change to FortiGate Security Group and add RDP and ICMP to the Security Group

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair

Select a key pair

AWS-Lab | RSA

☑ I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

Cancel **Launch Instances**

Figure 10.131: Accept key pair and launch instances

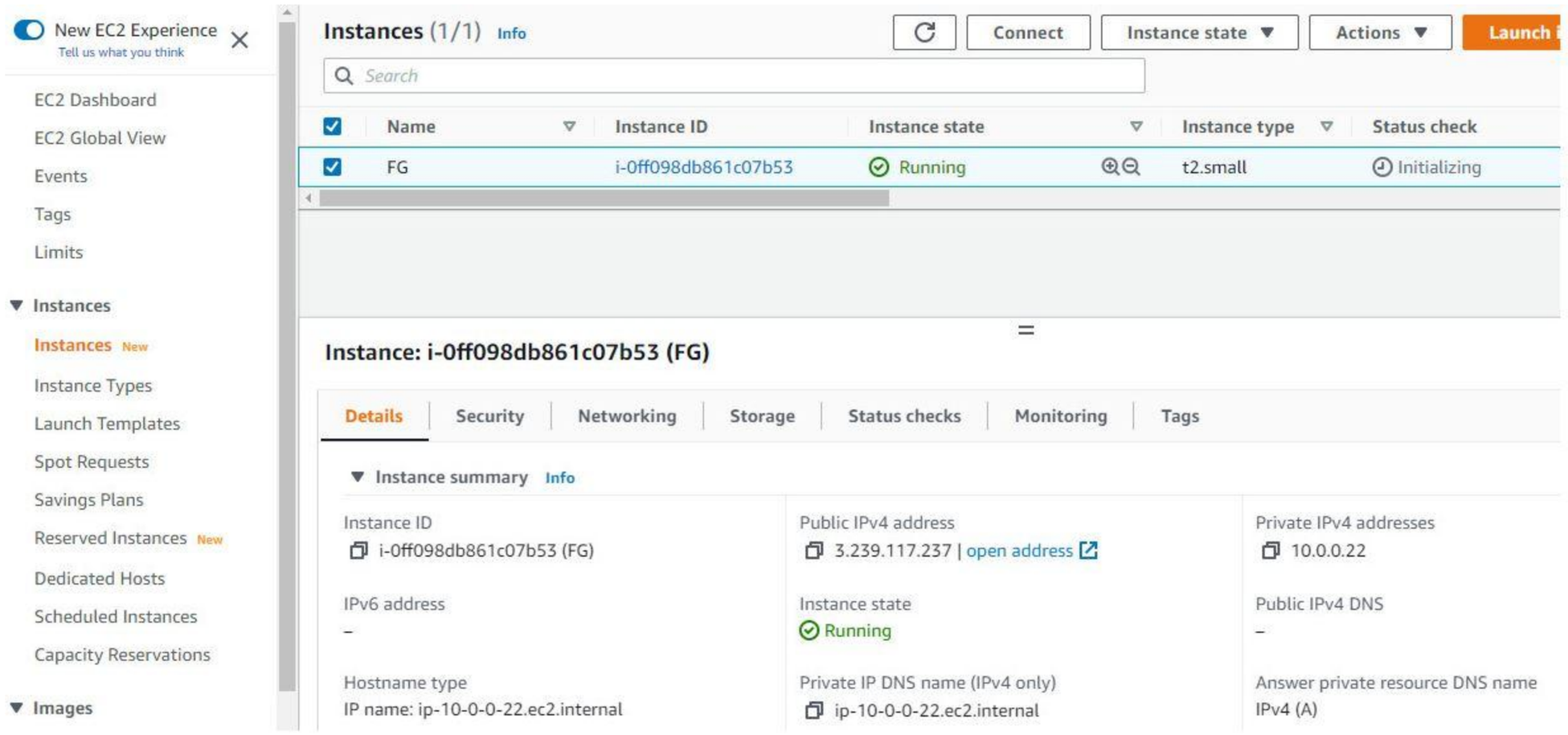

Figure 10.132: FG instance has been launched successfully

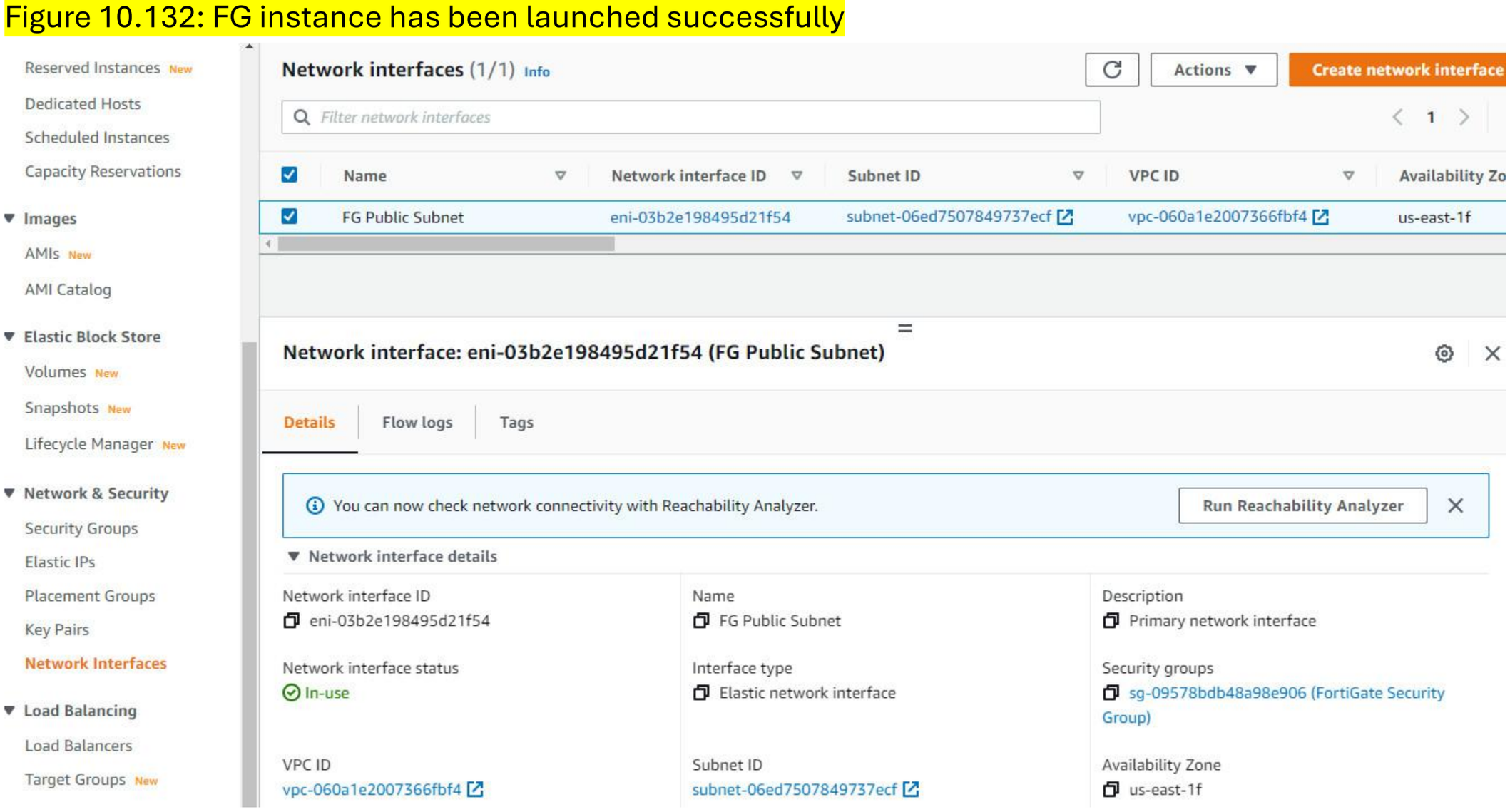

Figure 10.133: Change default interface name to FG Public Subnet

7. Add a new private subnet interface.

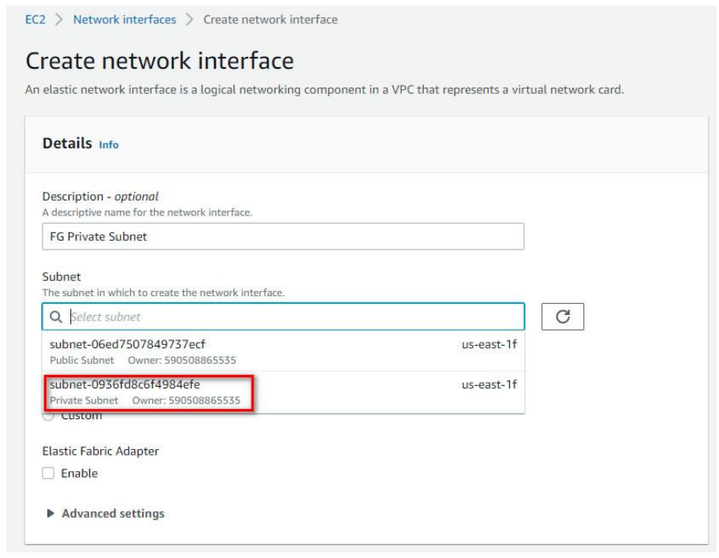

Figure 10.134: Create FG Private Subnet

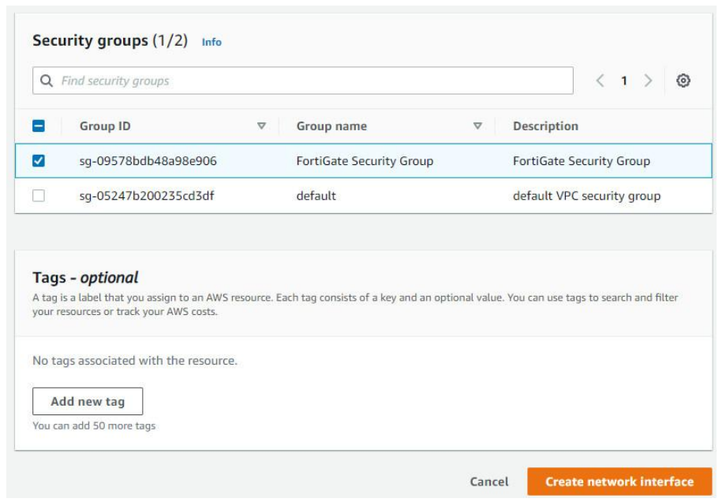

Figure 10.135: Create FG Private Subnet

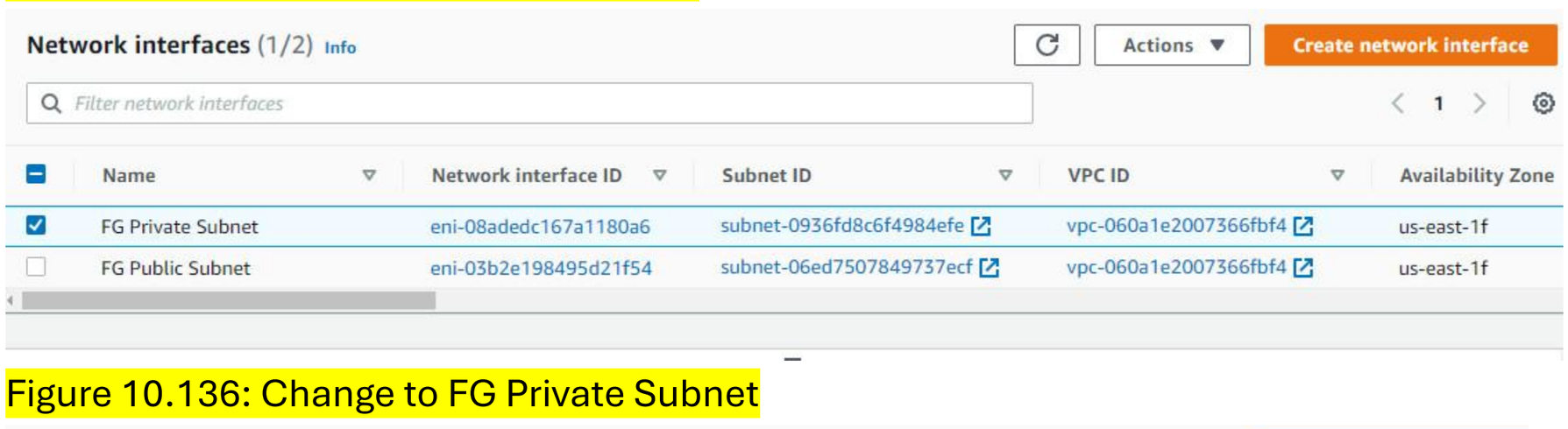

Figure 10.136: Change to FG Private Subnet

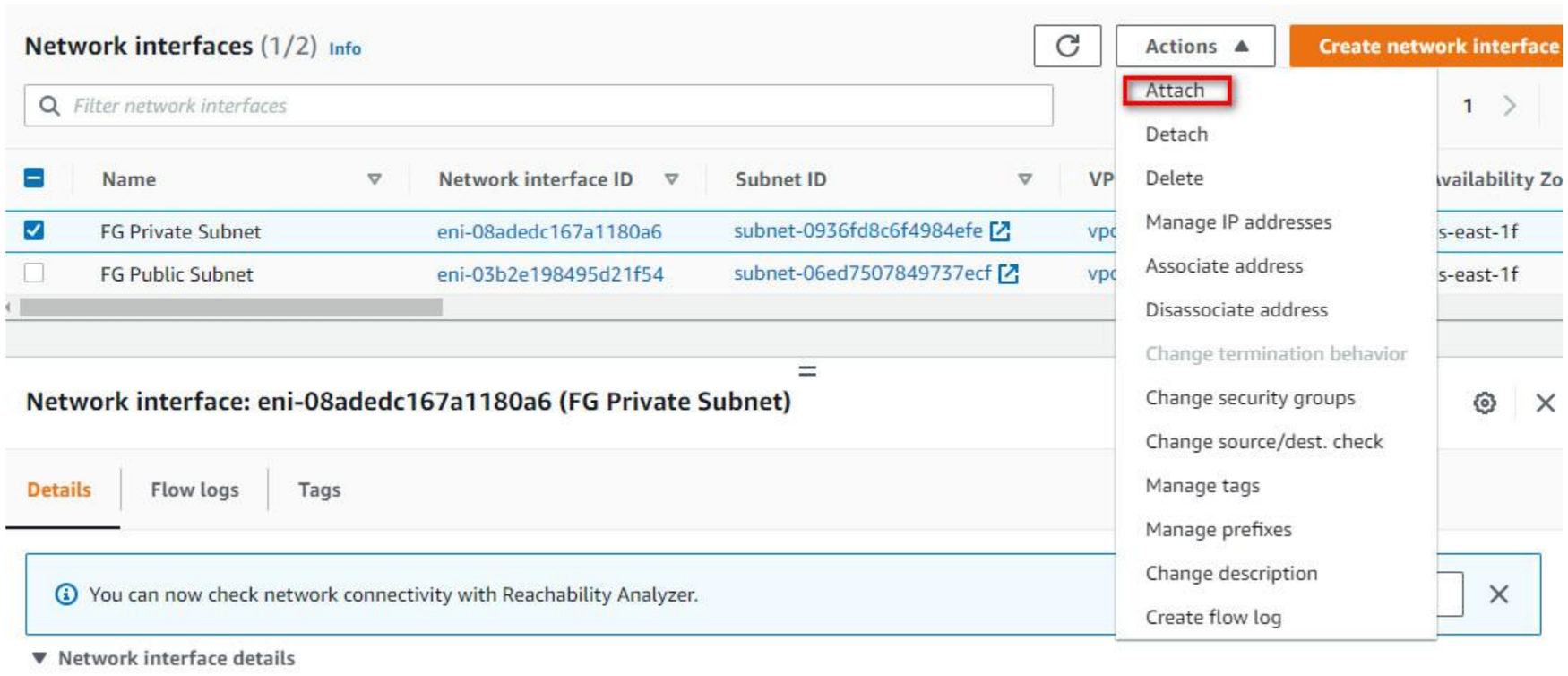

Figure 10.137: Attach the FG Private Subnet to FG

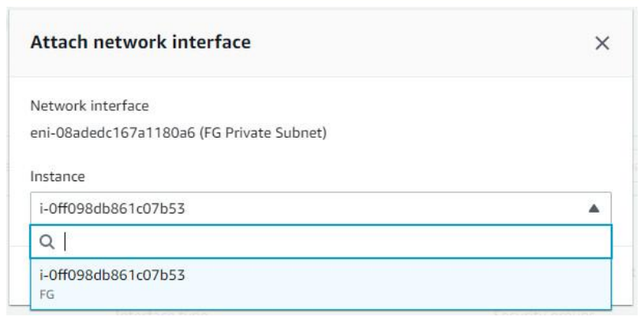

Figure 10.138: Attach the FG Private Subnet to FG

8. Disable Source and Destination check on both FG Private and Public Subnet.

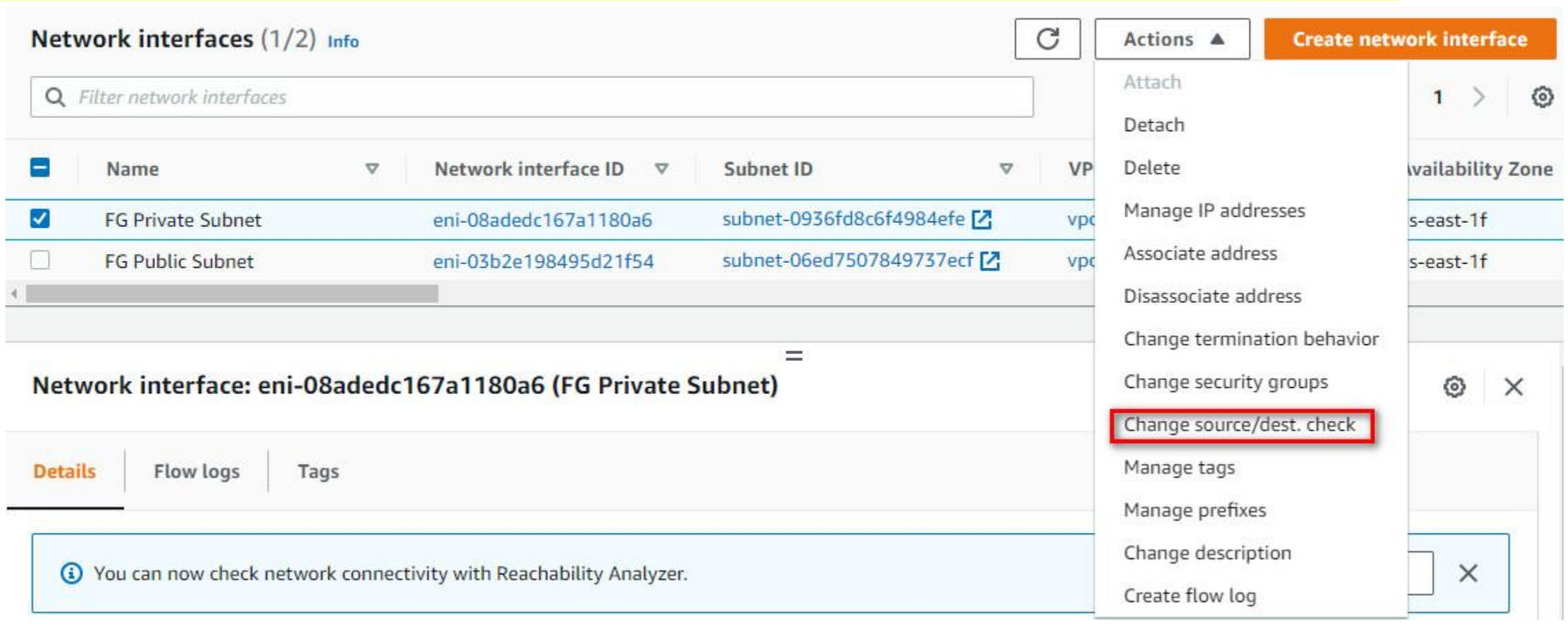

Figure 10.139: Disable source/destination check on FG Private Subnet

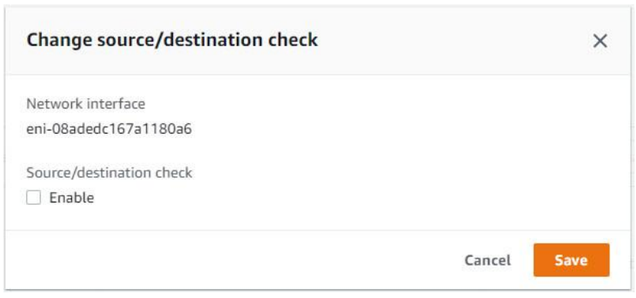

Figure 10.140: Disable source/destination check on FG Private Subnet

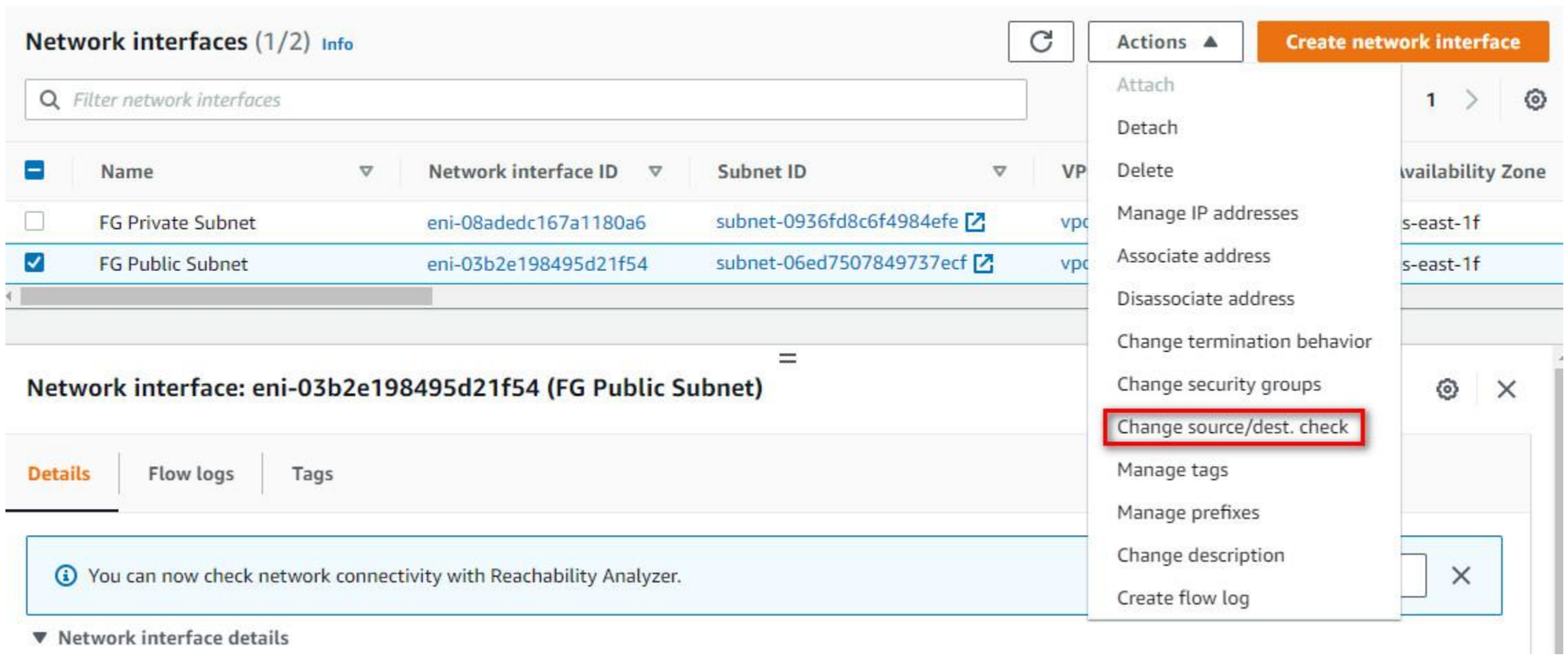

Figure 10.141: Disable source/destination check on FG Public Subnet

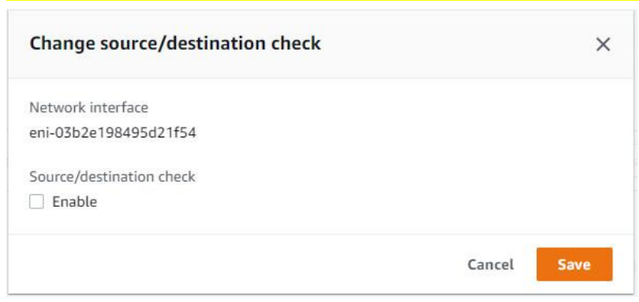

Figure 10.142: Disable source/destination check on FG Public Subnet

9. Edit private route table.

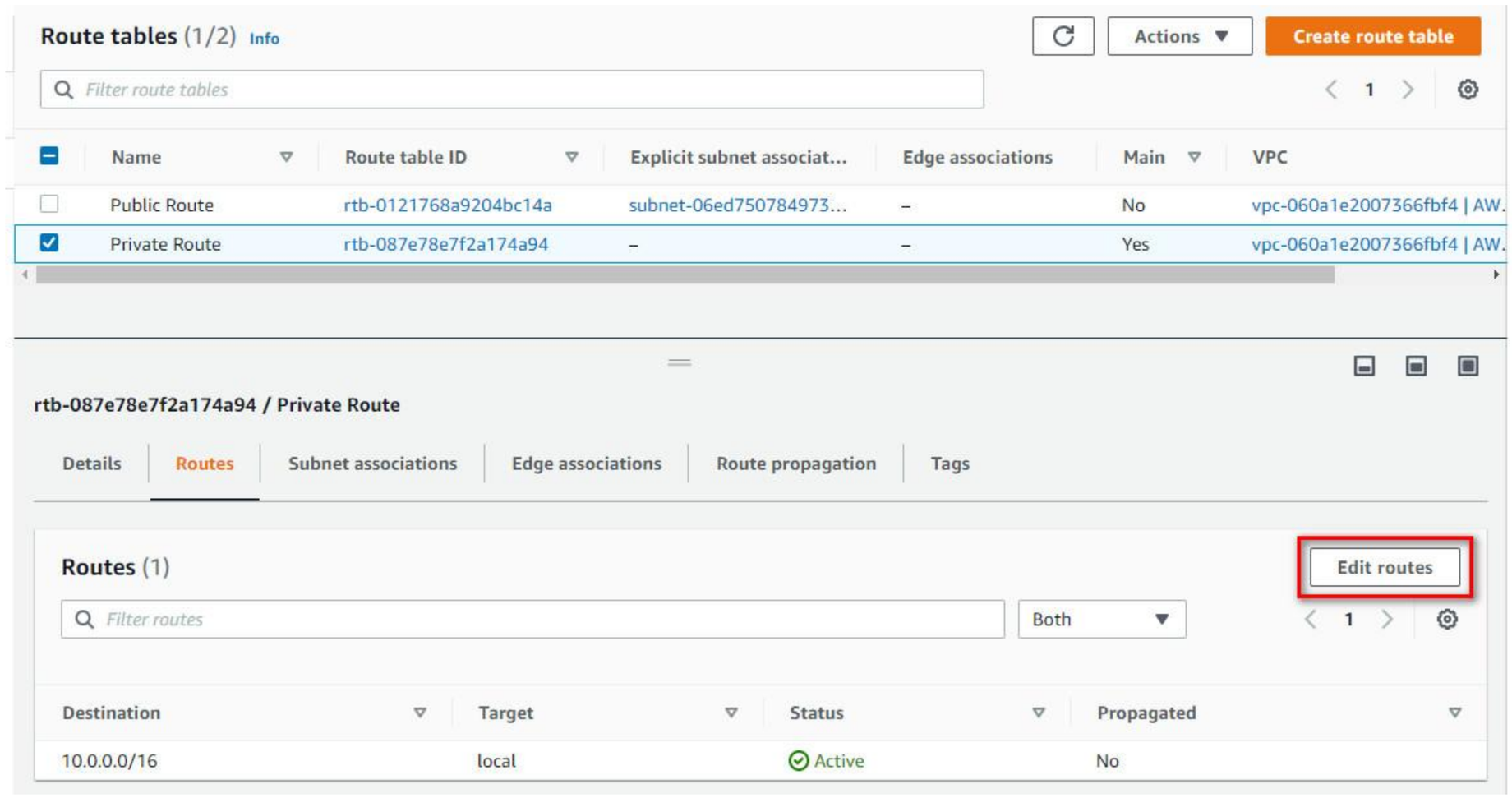

Figure 10.143: Edit Private Route

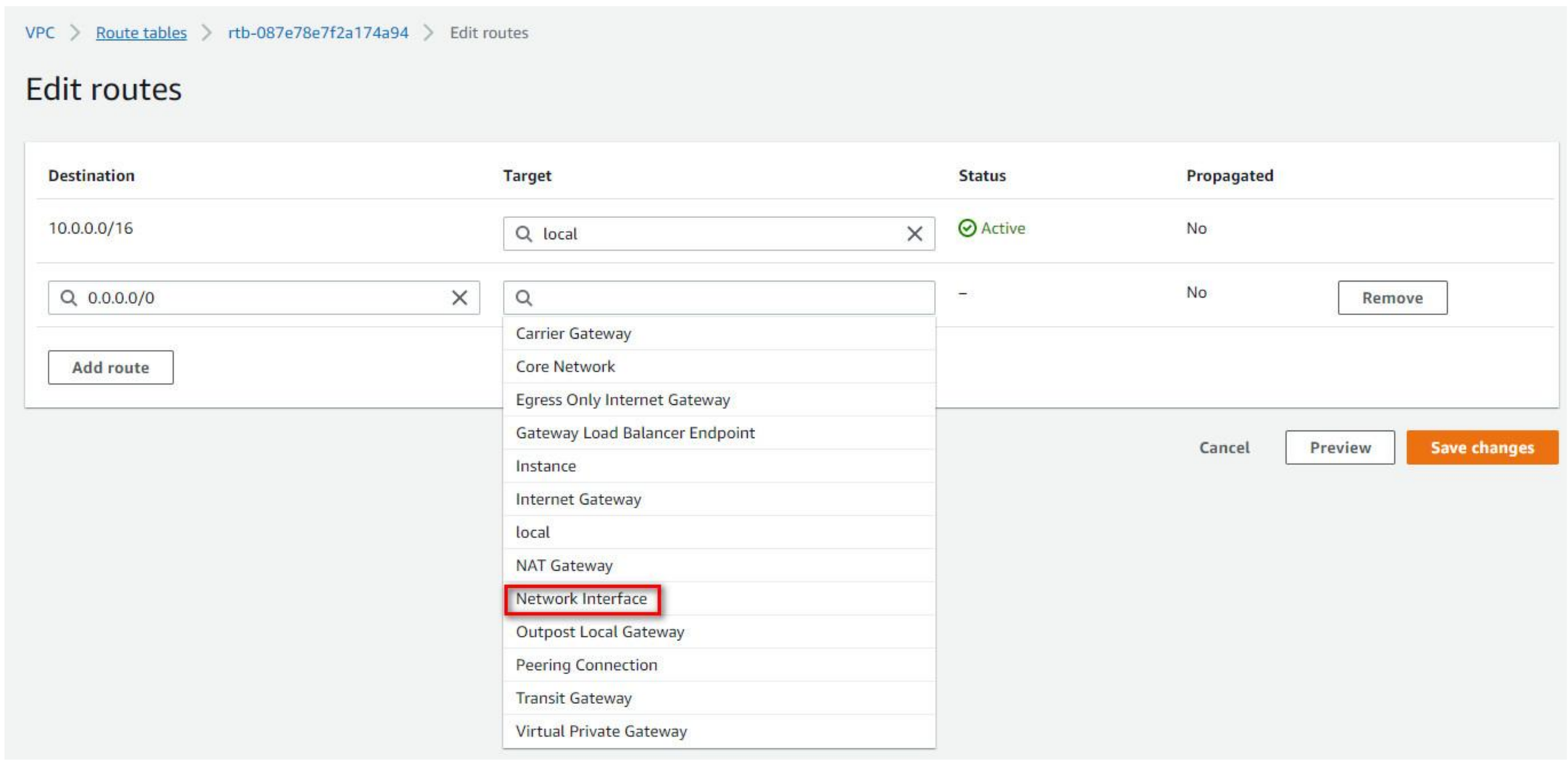

Figure 10.144: Add a default route and select Network Interface

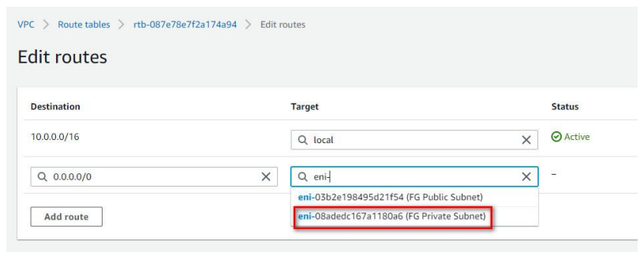

Figure 10.145: Add a default route to target FG Private Subnet

10. Verify Public and Private IP address of FG.

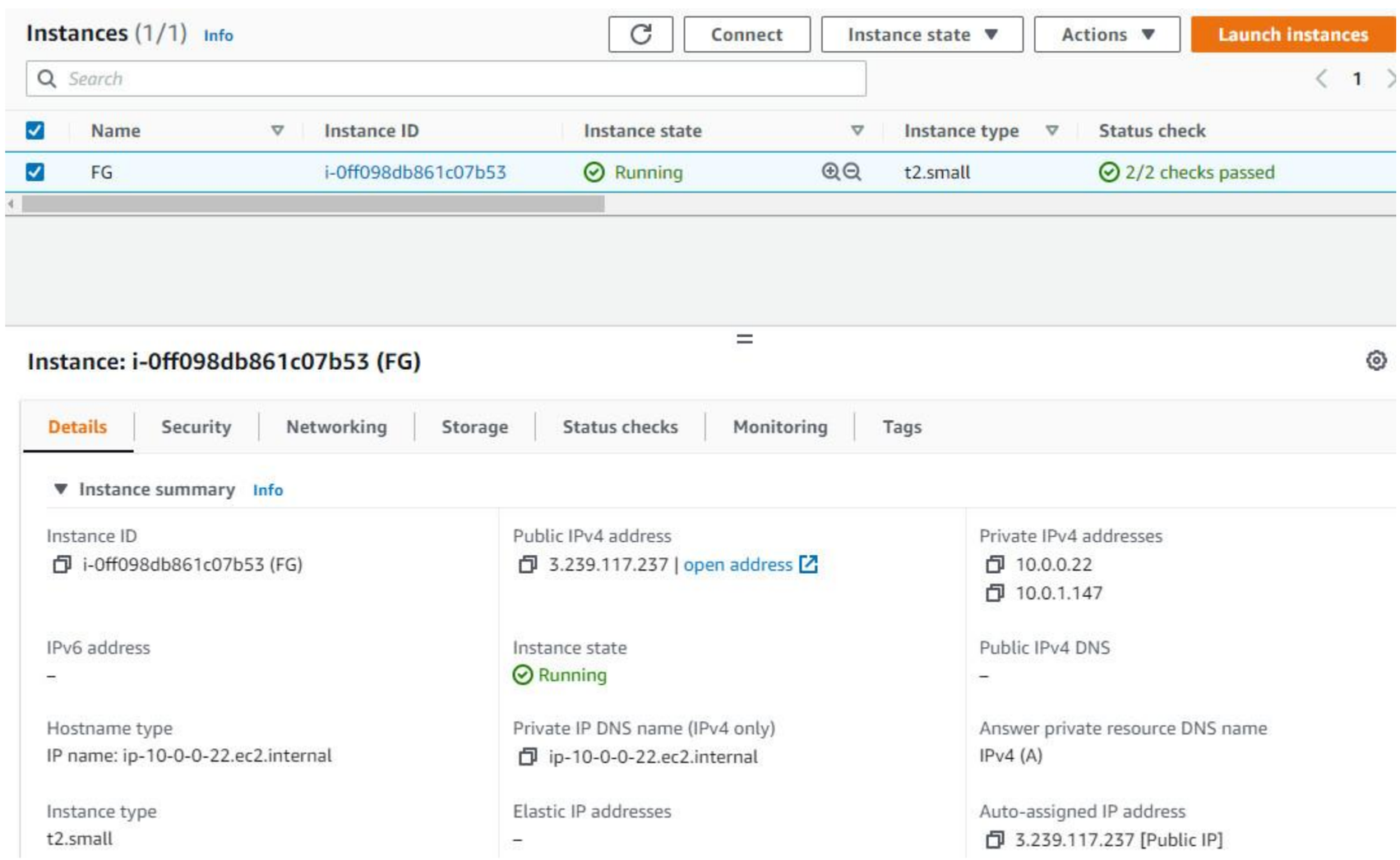

Figure 10.146: Verify public and private IP address of FG

11. Accessing FortiGate on AWS.Type the IP address in the browser. You should be able to see the FortiGate credentials page. Enter your username and password to login to the firewall.

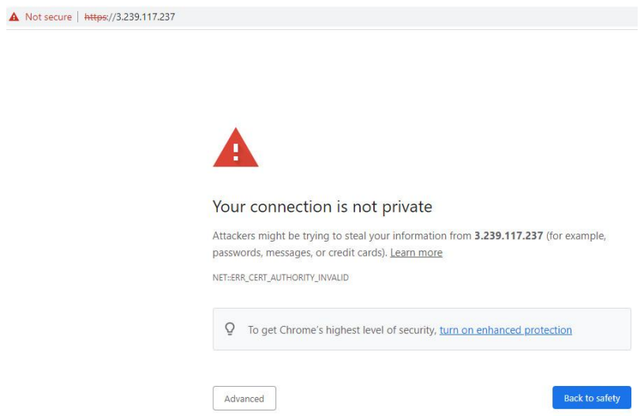

Figure 10.147: Access FortiGate

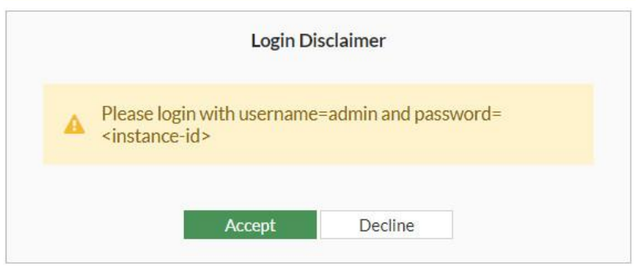

Figure 10.148: Access FortiGate

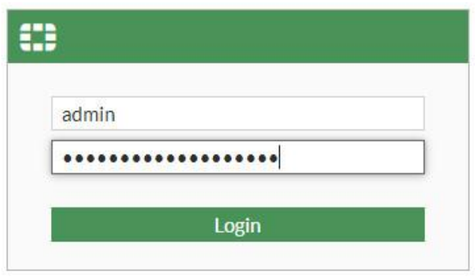

Figure 10.149: Username is admin and password is instance ID of FortiGate

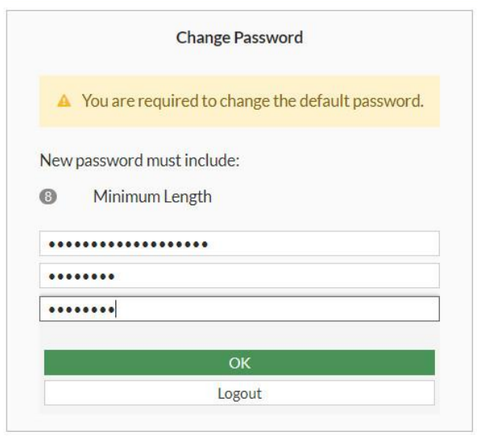

Figure 10.150: Change password

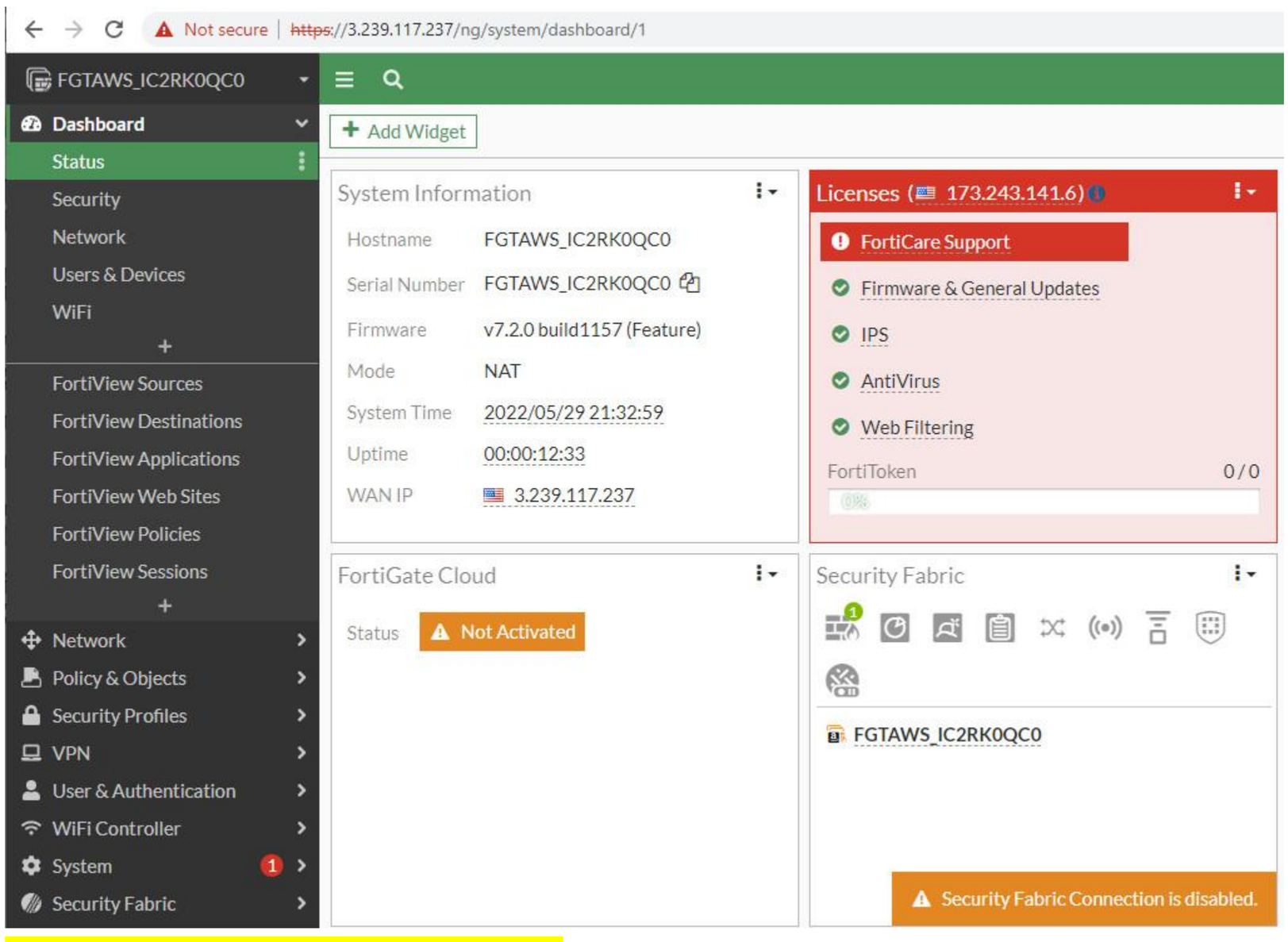

Figure 10.151: FortiGate dashboard

You should set port1 and port2 as DHCP client to receive an IP address from External and LAN subnet. Port1 is belong to External subnet or the internet and port2 is belong to the LAN.

Table 10.5: Port1 and Port2 description

Subnet	Description
Port1	External subnet used to connect the FortiGate-VM to the internet.
Port2	LAN subnet used to deploy services.

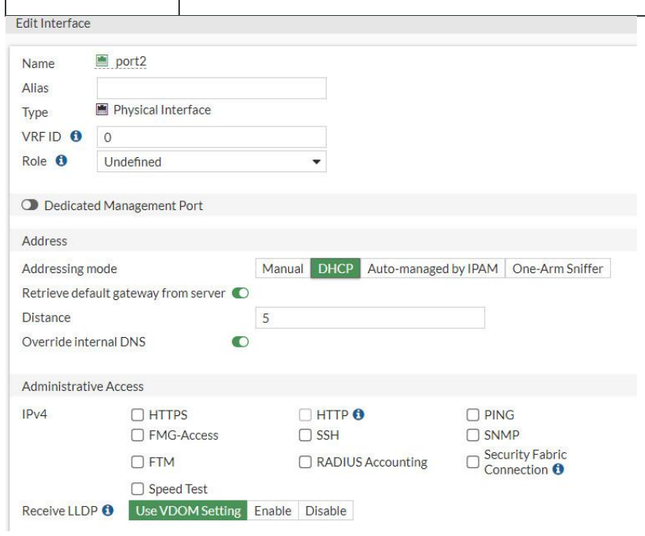

Figure 10.152: Change port2 to DHCP Client

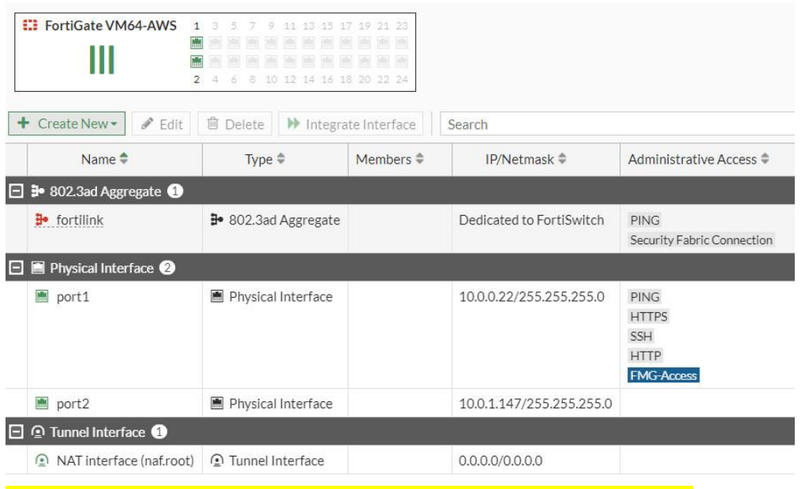

Figure 10.153: FortiGate interfaces