

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.

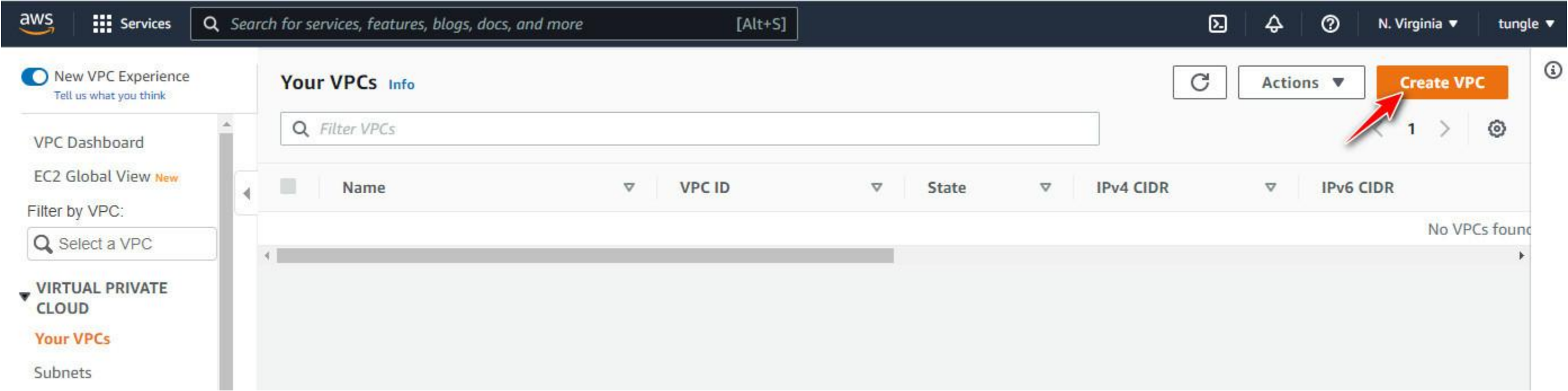


Figure 10.107: Create a VPC

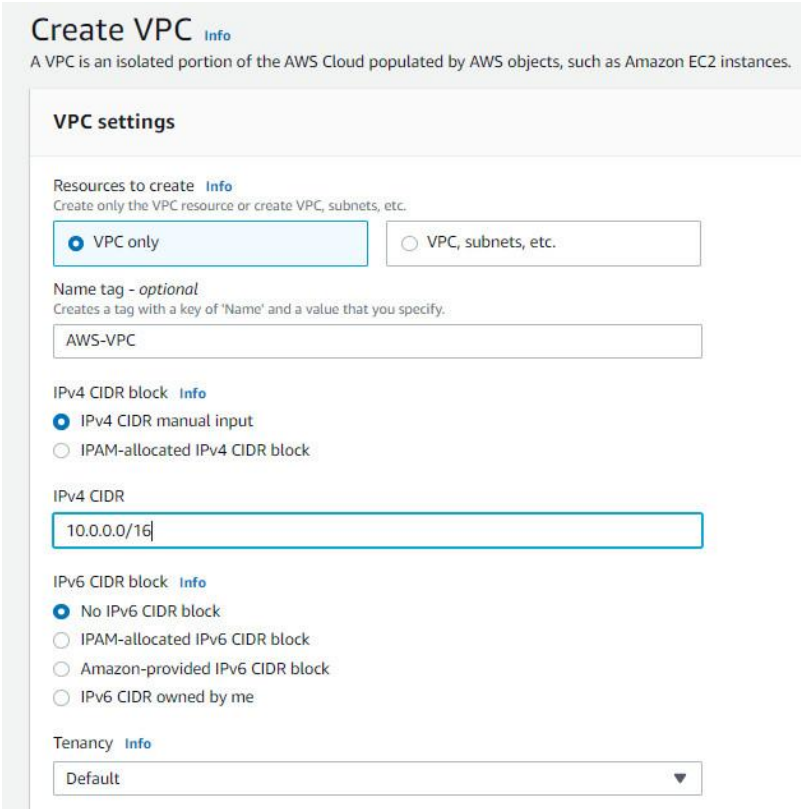


Figure 10.108: Create a VPC named “AWS-VPC”

2. Create a subnet.

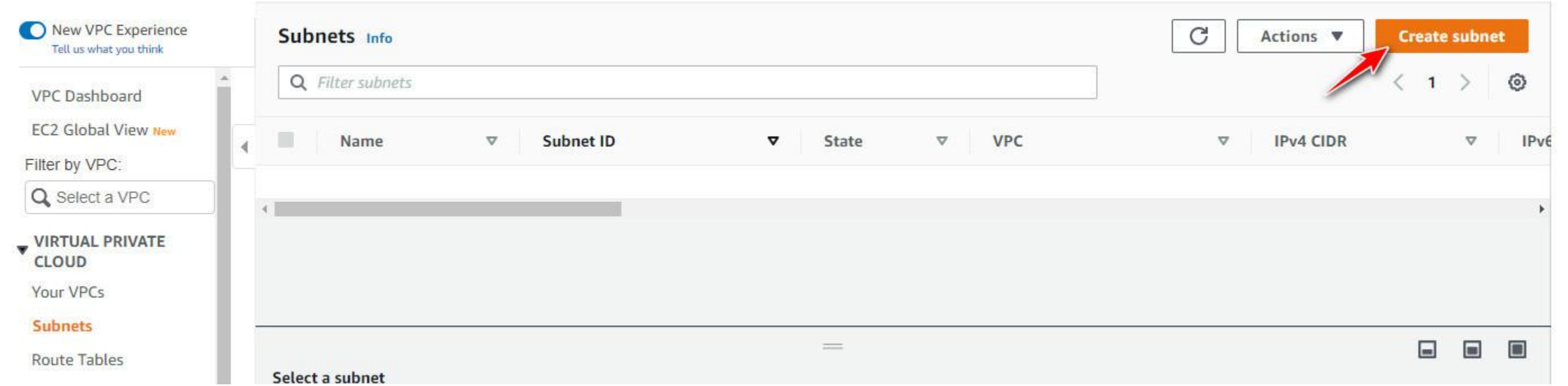


Figure 10.109: Create a subnet

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-060a1e2007366fbf4 (AWS-VPC) ▼

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Public Subnet
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference ▼

IPv4 CIDR block Info
10.0.0.0/24 ✕

Figure 10.110: Create a public subnet under AWS-VPC

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-060a1e2007366fbf4 (AWS-VPC) ▼

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Private Subnet
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference ▼

IPv4 CIDR block Info
10.0.1.0/24 ✕

Figure 10.111: Create a private subnet under AWS-VPC

3. Create an internet gateway.

New VPC Experience
Tell us what you think

VPC Dashboard

EC2 Global View New

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Internet gateways Info

Filter internet gateways

	Name	Internet gateway ID	State	VPC ID	Owner
No internet gateways found in this Region					

Select an internet gateway above

Actions ▼

Create internet gateway

Figure 10.112: Create an internet gateway

VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Create a tag with a key of 'Name' and a value that you specify.
AWS-IGW

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
Name	AWS-IGW	Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

Figure 10.113: Create an internet gateway

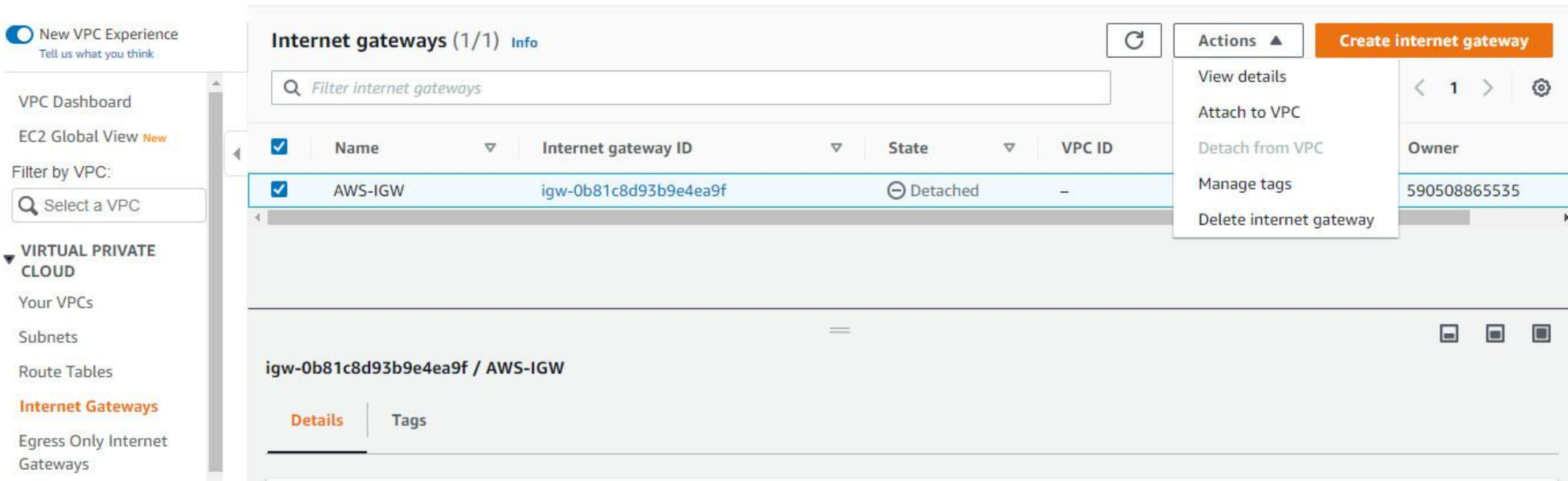


Figure 10.114: Attach an internet gateway to VPC

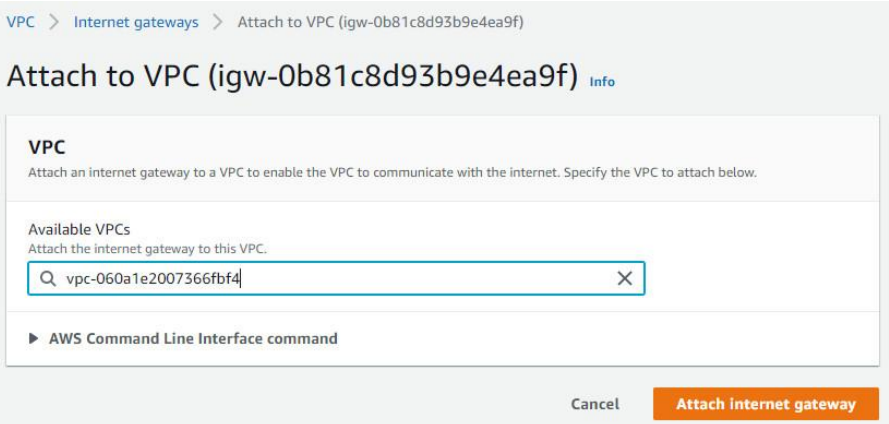


Figure 10.115: Attach an internet gateway to VPC

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

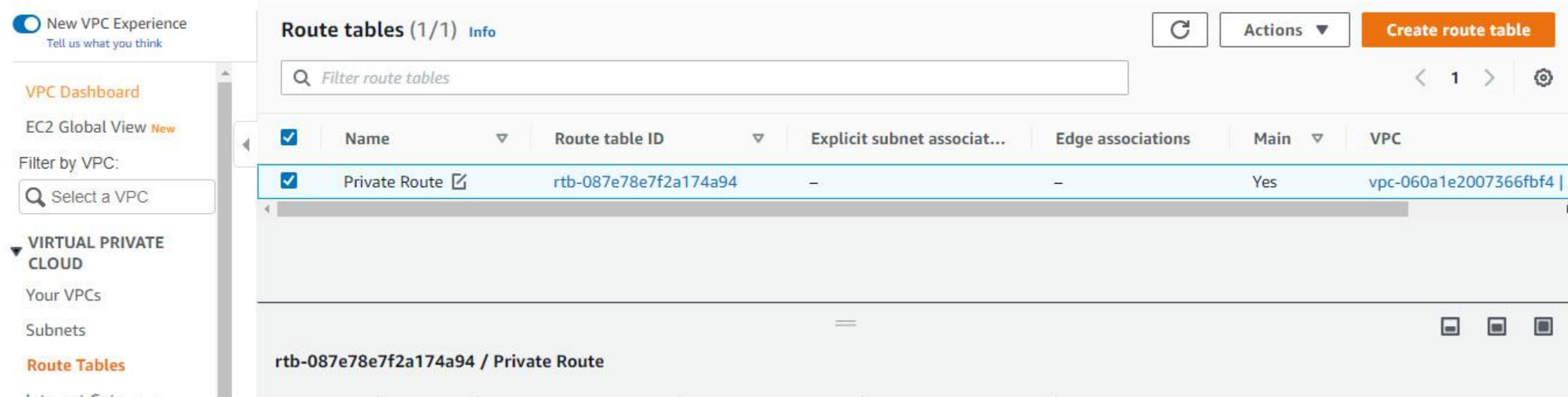


Figure 10.116: Edit private route

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

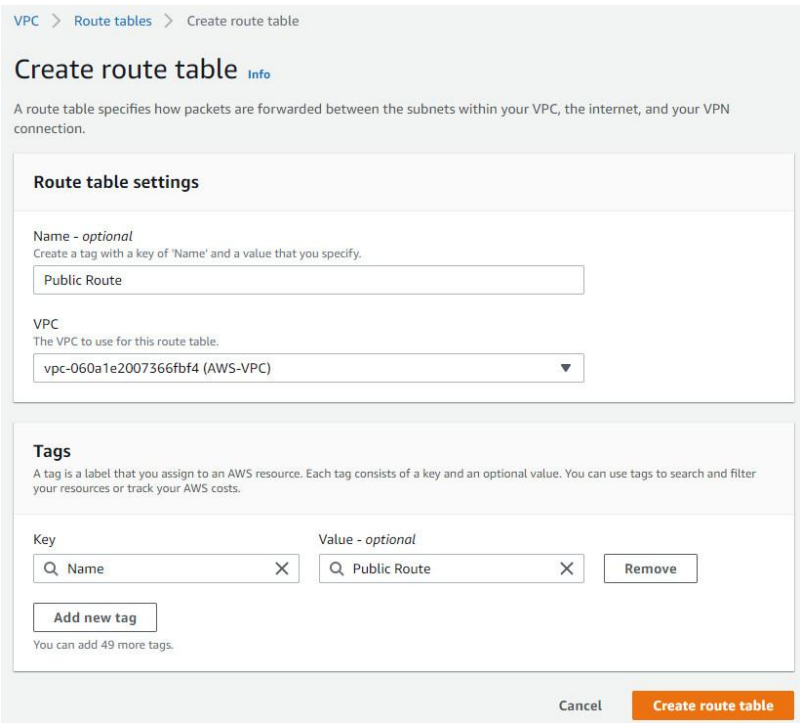


Figure 10.117: Create a public route

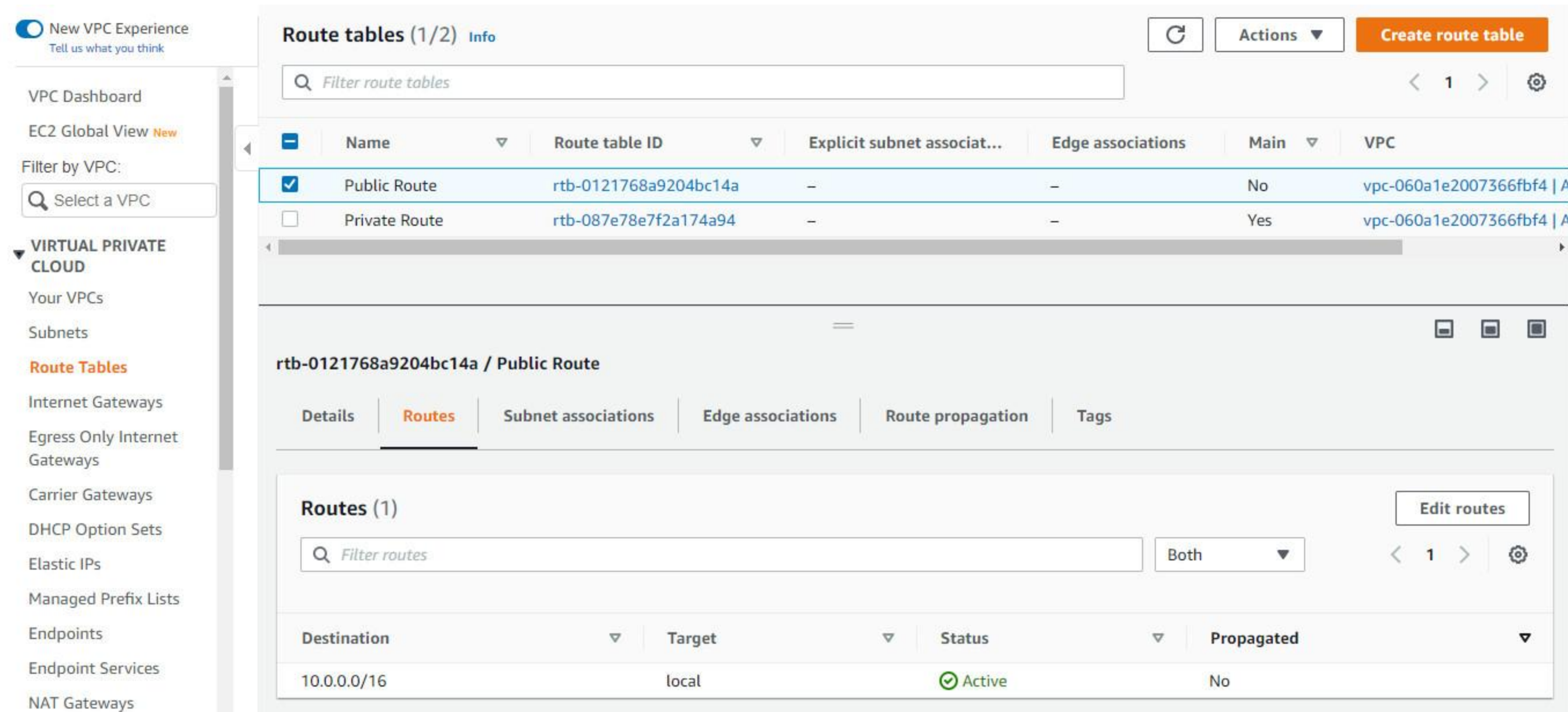


Figure 10.118: Edit routes on Public Route

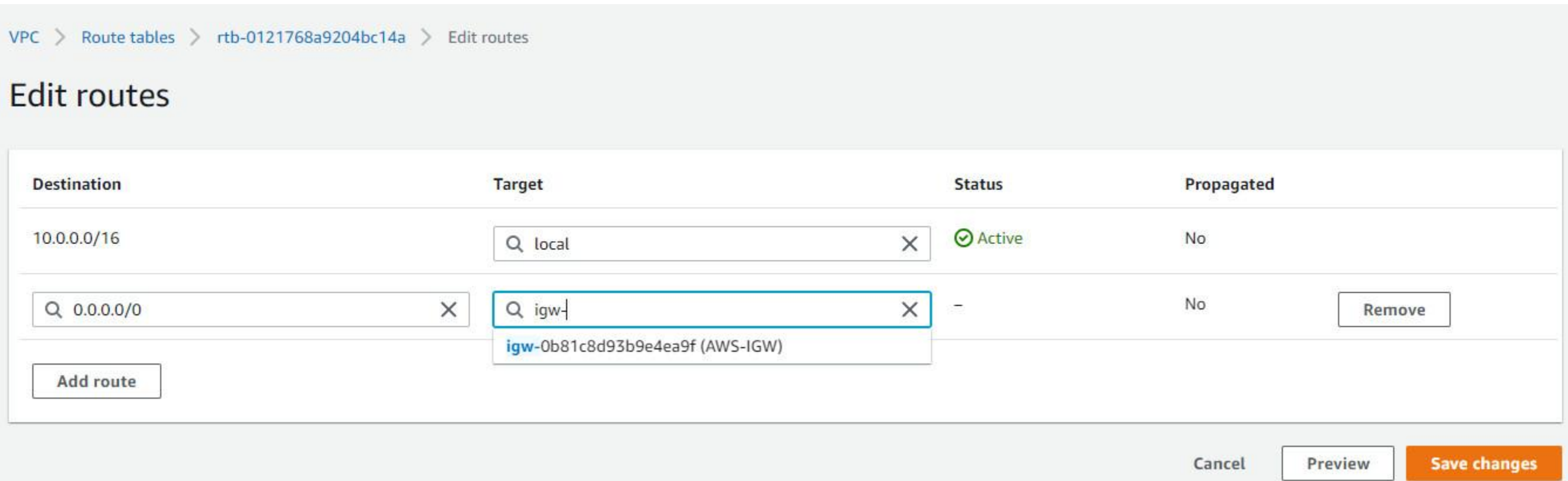


Figure 10.119: Create a new default route to the internet gateway

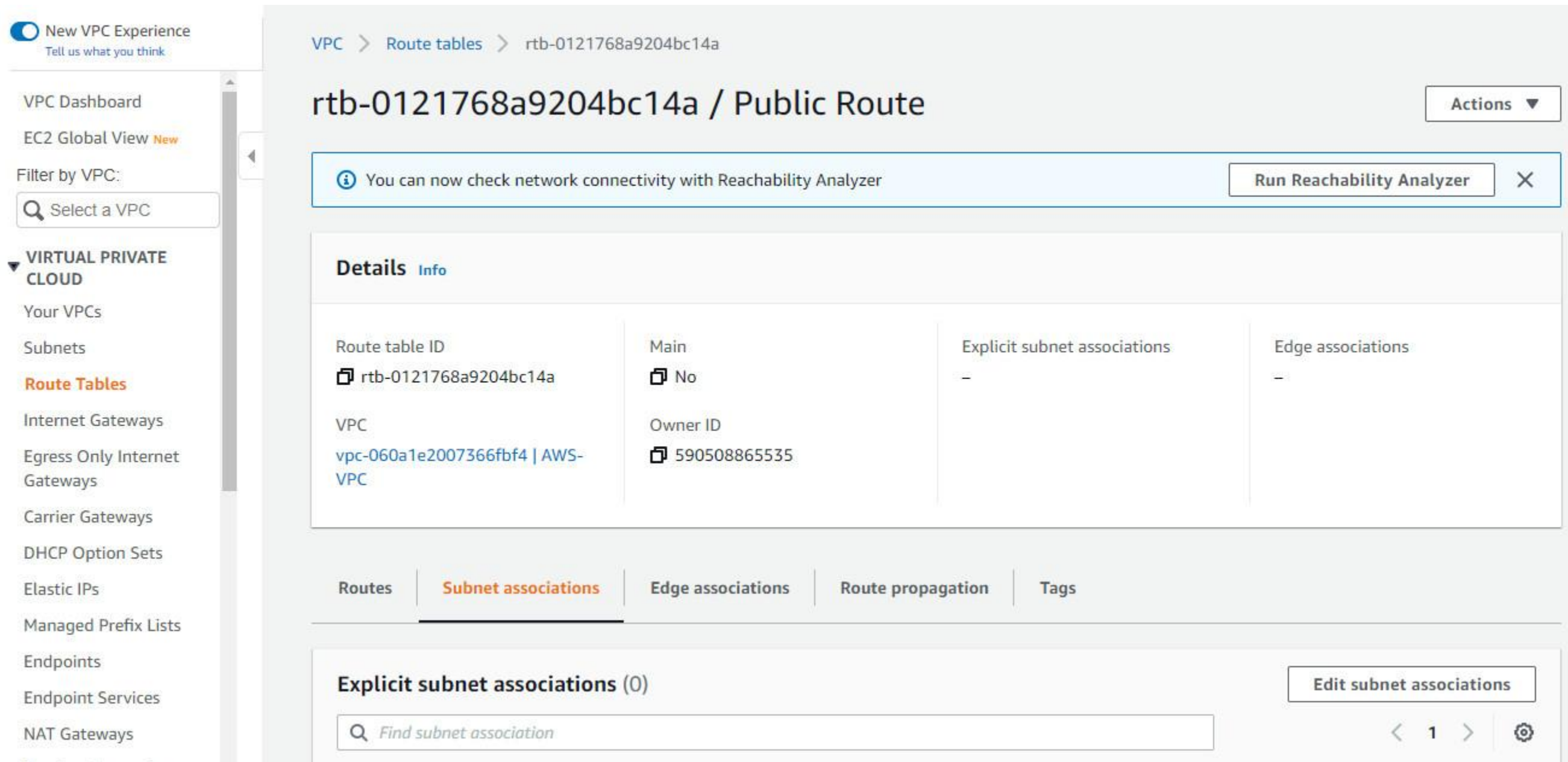


Figure 10.120: Associate Public Subnet to Public Route

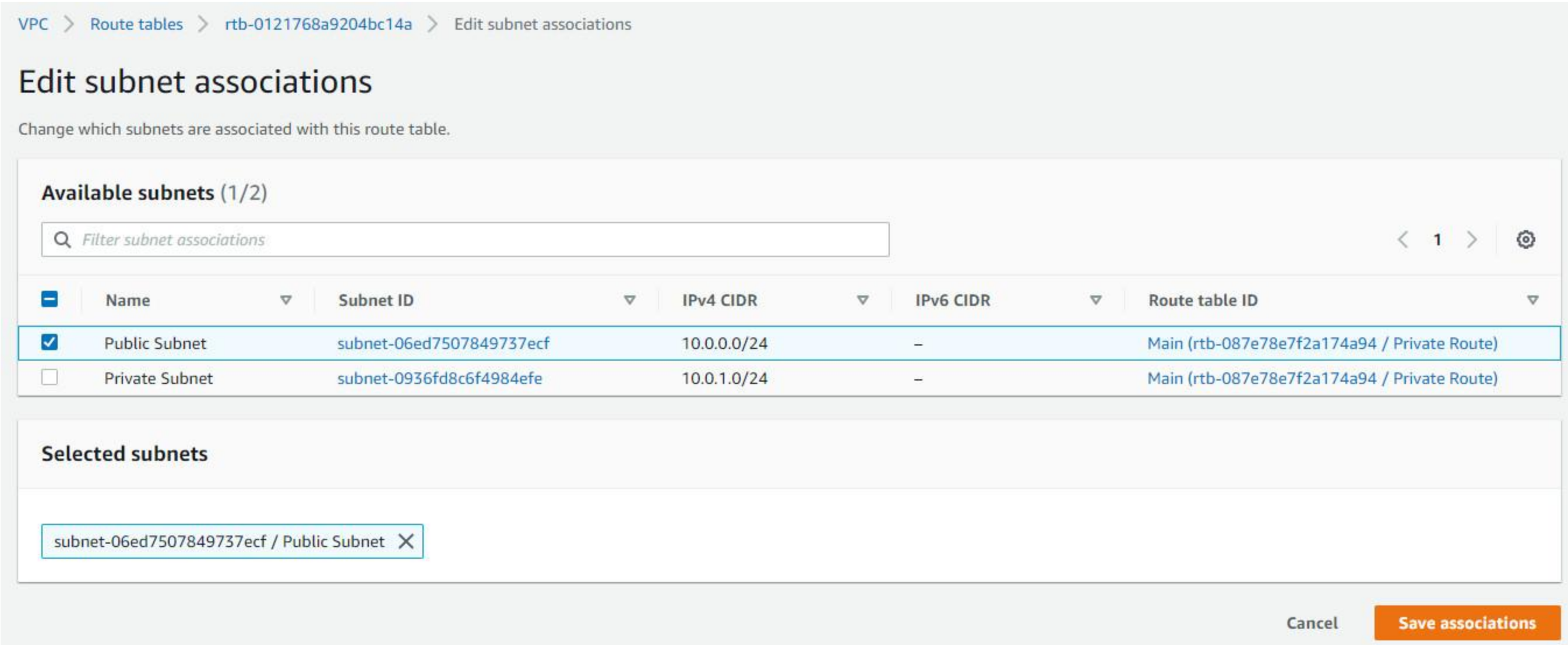


Figure 10.121: Associate Public Subnet to Public Route

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

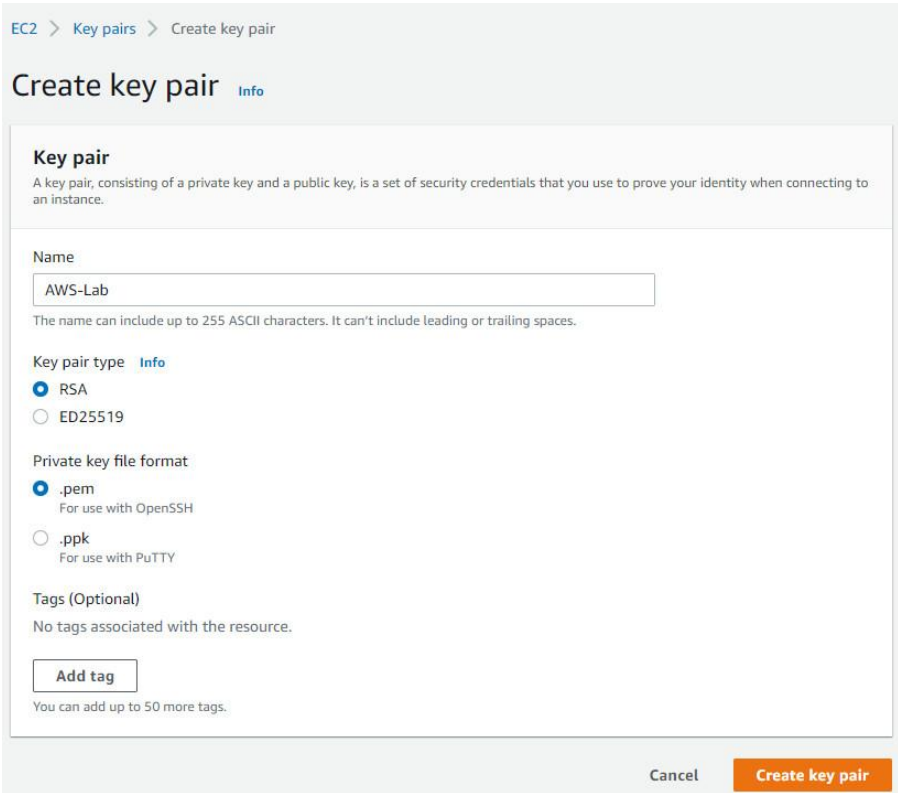


Figure 10.122: Create a key pair

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

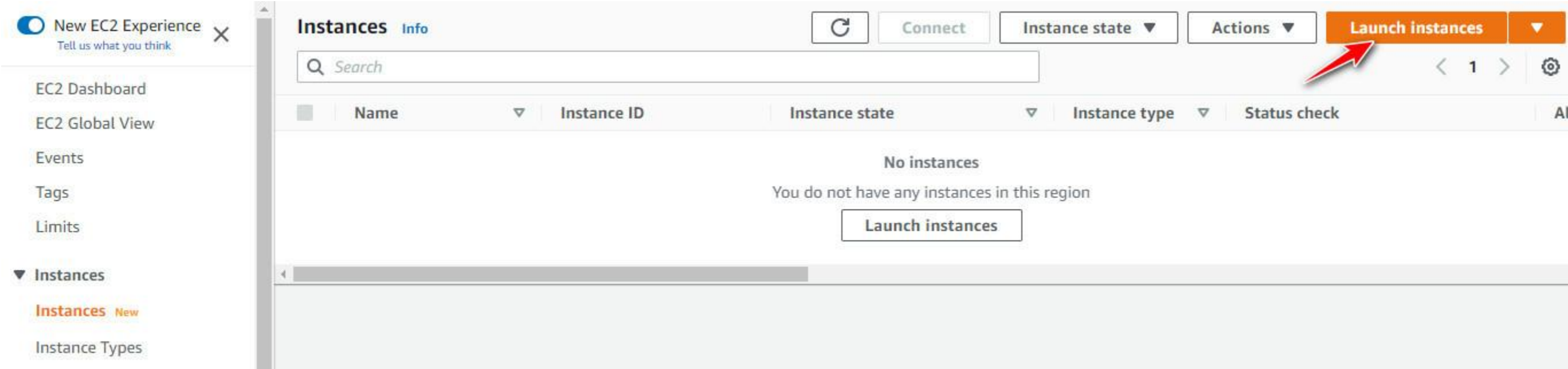


Figure 10.123: Launch a FortiGate instance

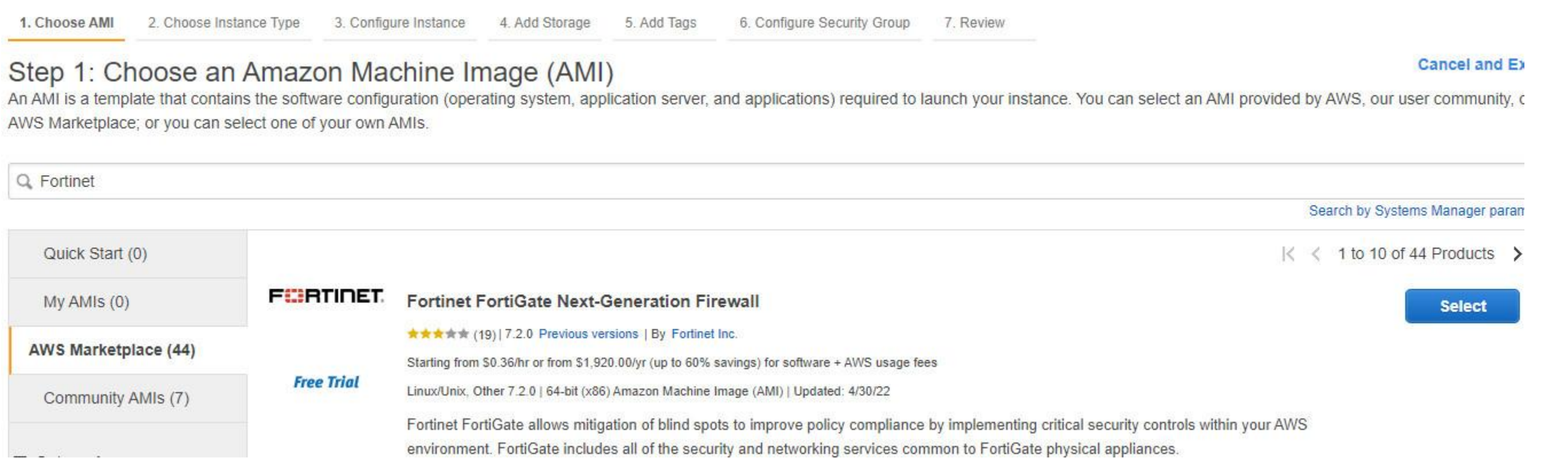



Figure 10.124: Select Fortinet FortiGate Next-Generation Firewall



Fortinet FortiGate Next-Generation Firewall

FortiGate Next-Generation Firewall technology delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features. Application control, antivirus, IPS, Web filtering and VPN along with advanced features such as an extreme threat database, vulnerability management and flow-based ...

[More info](#)

[View Additional Details in AWS Marketplace](#)

Fortinet FortiGate Next-Generation Firewall

FortiGate Next-Generation Firewall technology delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features. Application control, antivirus, IPS, Web filtering and VPN along with advanced features such as an extreme threat database, vulnerability management and flow-based ...

[More info](#)

[View Additional Details in AWS Marketplace](#)

Pricing Details

Instance Type	Software	EC2	Total
t2.small	\$0.36	\$0.023	\$0.383/hr
t3.small	\$0.88	\$0.021	\$0.901/hr
t3.xlarge	\$1.02	\$0.166	\$1.186/hr
c4.large	\$0.88	\$0.10	\$0.98/hr
c4.xlarge	\$1.02	\$0.199	\$1.219/hr
c4.2xlarge	\$2.35	\$0.398	\$2.748/hr
c4.4xlarge	\$3.29	\$0.796	\$4.086/hr
c4.8xlarge	\$4.10	\$1.591	\$5.691/hr
c5.large	\$0.88	\$0.085	\$0.965/hr
c5.xlarge	\$1.02	\$0.17	\$1.19/hr
c5.2xlarge	\$2.35	\$0.34	\$2.69/hr
c5.4xlarge	\$3.29	\$0.68	\$3.97/hr
c5.9xlarge	\$4.10	\$1.53	\$5.63/hr
c5.18xlarge	\$5.16	\$3.06	\$8.22/hr
c5d.large	\$0.88	\$0.096	\$0.976/hr
c5d.xlarge	\$1.02	\$0.192	\$1.212/hr
c5d.2xlarge	\$2.35	\$0.384	\$2.734/hr

Product Details

By	Fortinet Inc.
Customer Rating	★★★★★ (19)
Latest Version	7.2.0
Base Operating System	Linux/Unix, Other 7.2.0
Delivery Method	64-bit (x86) Amazon Machine Image (AMI)
License Agreement	End User License Agreement
On Marketplace Since	11/7/14

Highlights

- FortiGate offers protection from a broad array of threats, with support for all of the security and networking services offered by the FortiOS operating

[Cancel](#)
[Continue](#)

Figure 10.125: Accept FortiGate licence

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications, scale horizontally to increase capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types.

Filter by:

All instance families

Current generation

Show/Hide Columns

Currently selected: t2.small (- ECUs, 1 vCPUs, 2.5 GHz, -, 2 GiB memory, EBS only)

Note: The vendor recommends using a **c6i.xlarge** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)
	t2	t2.nano	1	0.5	EBS only
	t2	t2.micro Free tier eligible	1	1	EBS only
	t2	t2.small	1	2	EBS only
	t2	t2.medium	2	4	EBS only
	t2	t2.large	2	8	EBS only

Figure 10.126: Select FortiGate instance type

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or [create a new default VPC](#).

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of, and more.

Number of instances ⓘ

1

Launch into Auto Scaling Group ⓘ

Purchasing option ⓘ

☐ Request Spot instances

Network ⓘ

vpc-060a1e2007366fbf4 | AWS-VPC ⓘ

Create new VPC ⓘ

No default VPC found. [Create a new default VPC](#).

Subnet ⓘ

subnet-06ed7507849737ecf | Public Subnet | us-east-1 ⓘ

Create new subnet ⓘ

251 IP Addresses available

Auto-assign Public IP ⓘ

Enable ⓘ

Hostname type ⓘ

Use subnet setting (IP name) ⓘ

DNS Hostname ⓘ

☒ Enable IP name IPv4 (A record) DNS requests

☒ Enable resource-based IPv4 (A record) DNS requests

☐ Enable resource-based IPv6 (AAAA record) DNS requests

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	<input type="text" value="2"/>	General Purpose SSD (gp2) ▾	100 / 3000	N/A
<div>EBS ▾</div>	<div>/dev/sdb ▾</div>	<div>Search (case-insensit</div>	<input type="text" value="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 ⓘ
<input type="text" value="Name"/>	<input type="text" value="FG"/>	<input checked="" type="checkbox"/>

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, if you want to allow 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 group.

Assign a security group:

☒ Create a new security group

☐ Select an existing security group

Security group name:

Description:

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

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

New EC2 Experience

Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

Instances (1/1)

Info

Connect

Instance state

Actions

Launch

Search

Name	Instance ID	Instance state	Instance type	Status check
FG	i-0ff098db861c07b53	Running	t2.small	Initializing

Instance: i-0ff098db861c07b53 (FG)

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

Instance summary

Info

Instance ID

i-0ff098db861c07b53 (FG)

Public IPv4 address

3.239.117.237 | open address

Private IPv4 addresses

10.0.0.22

IPv6 address

-

Instance state

Running

Public IPv4 DNS

-

Hostname type

-

Private IP DNS name (IPv4 only)

ip-10-0-0-22.ec2.internal

Answer private resource DNS name

IPv4 (A)

Figure 10.132: FG instance has been launched successfully

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Target Groups

Network interfaces (1/1)

Info

Filter network interfaces

1

Create network interface

Actions

Name	Network interface ID	Subnet ID	VPC ID	Availability Zone
FG Public Subnet	eni-03b2e198495d21f54	subnet-06ed7507849737ecf	vpc-060a1e2007366fbf4	us-east-1f

Network interface: eni-03b2e198495d21f54 (FG Public Subnet)

Details

Flow logs

Tags

You can now check network connectivity with Reachability Analyzer.

Run Reachability Analyzer

Network interface details

Network interface ID

eni-03b2e198495d21f54

Name

FG Public Subnet

Description

Primary network interface

Network interface status

In-use

Interface type

Elastic network interface

Security groups

sg-09578bdb48a98e906 (FortiGate Security Group)

VPC ID

vpc-060a1e2007366fbf4

Subnet ID

subnet-06ed7507849737ecf

Availability Zone

us-east-1f

Figure 10.133: Change default interface name to FG Public Subnet

7. Add a new private subnet interface.

EC2

Network interfaces

Create network interface

Create network interface

An elastic network interface is a logical networking component in a VPC that represents a virtual network card.

Details

Info

Description - optional

A descriptive name for the network interface.

FG Private Subnet

Subnet

The subnet in which to create the network interface.

select subnet

subnet-06ed7507849737ecf

Public Subnet

Owner: 590508865535

us-east-1f

subnet-0936fd8c6f4984efe

Private Subnet

Owner: 590508865535

us-east-1f

Elastic Fabric Adapter

Enable

Advanced settings

Figure 10.134: Create FG Private Subnet

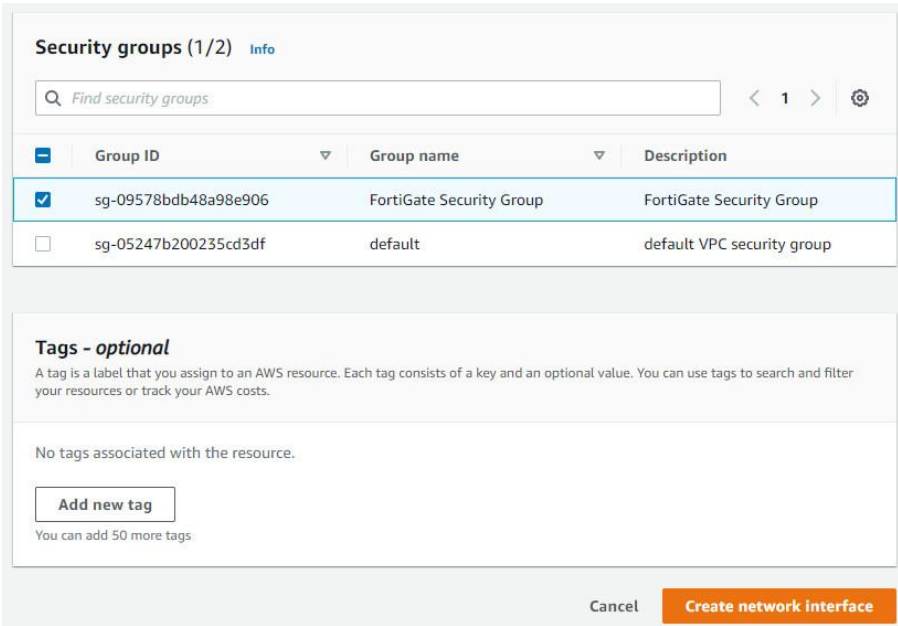


Figure 10.135: Create FG Private Subnet

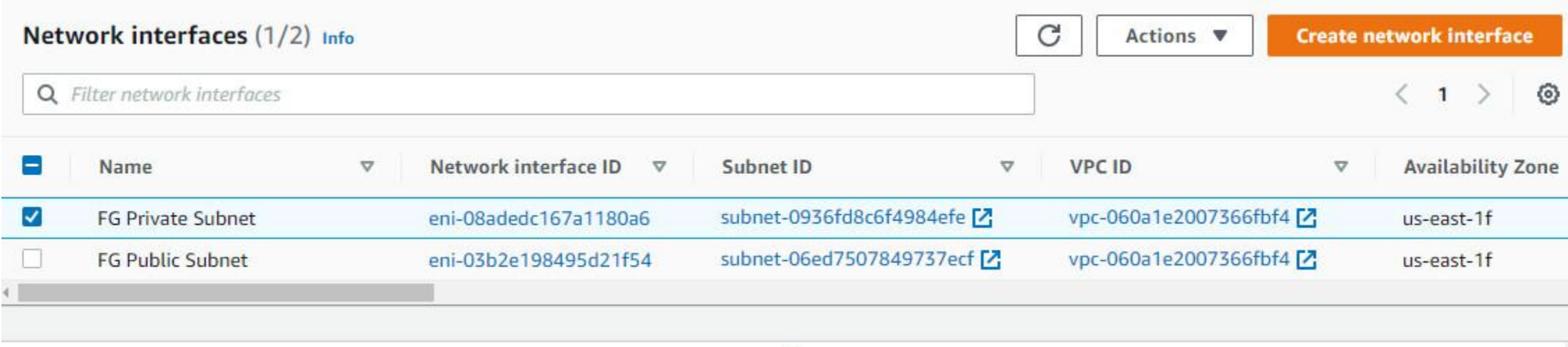


Figure 10.136: Change to FG Private Subnet

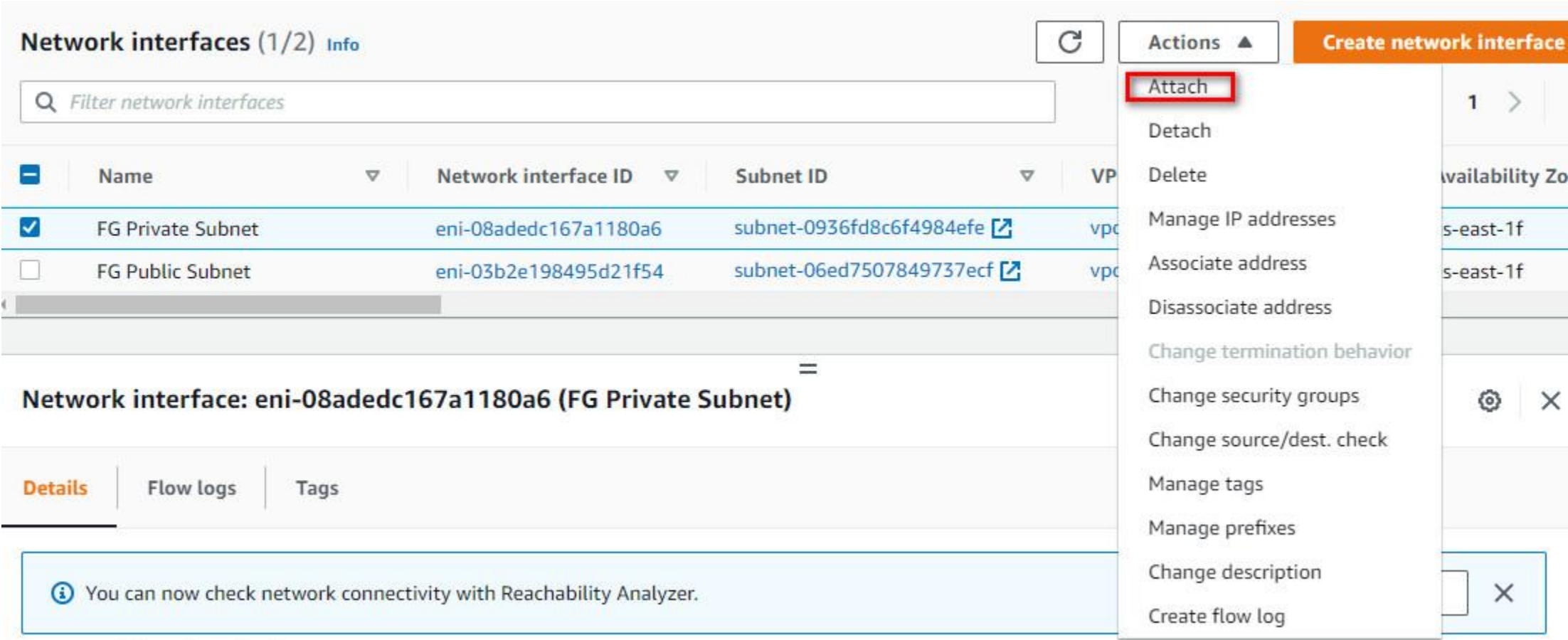


Figure 10.137: Attach the FG Private Subnet to FG

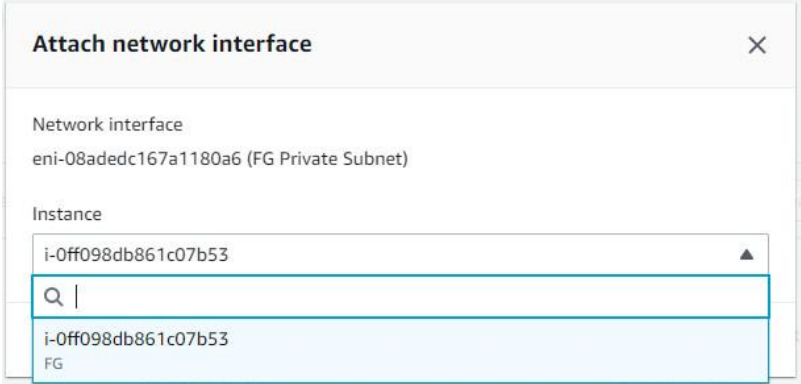


Figure 10.138: Attach the FG Private Subnet to FG

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

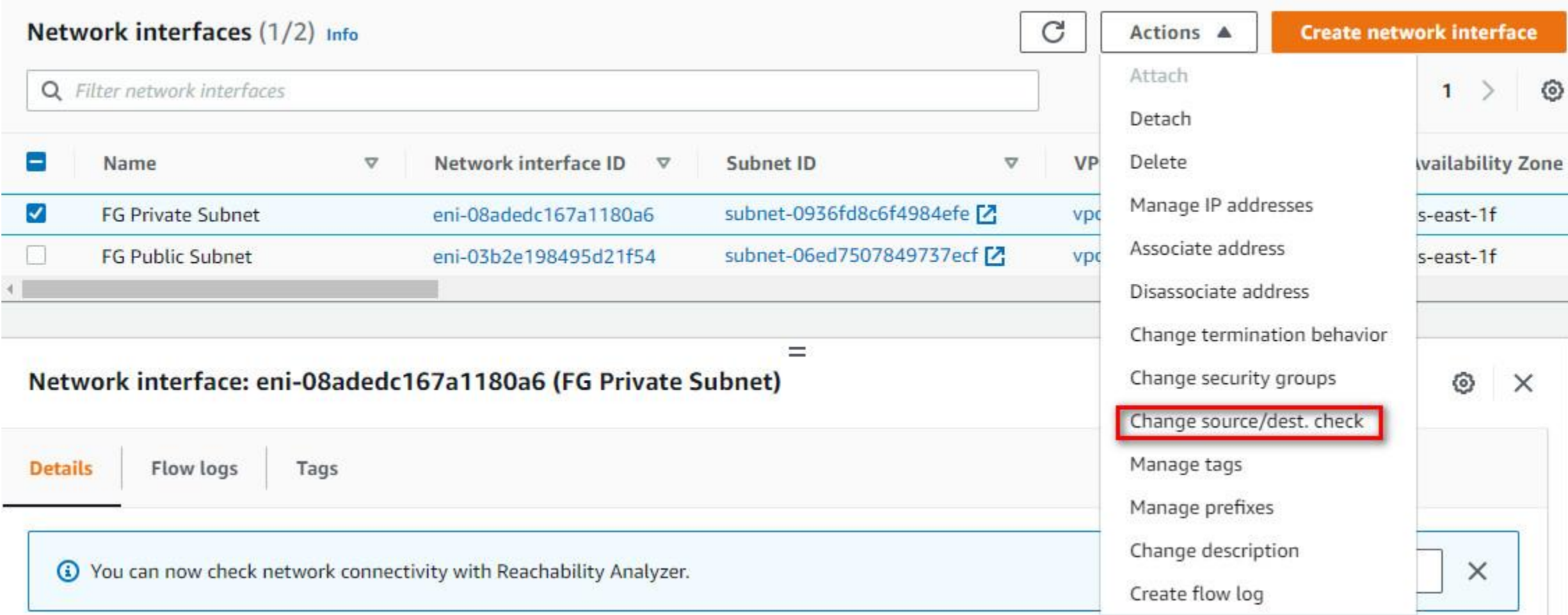


Figure 10.139: Disable source/destination check on FG Private Subnet

Change source/destination check

Network interface

eni-08adedc167a1180a6

Source/destination check

☐ Enable

Cancel

Save

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

Network interfaces (1/2) Info

Filter network interfaces

	Name	Network interface ID	Subnet ID	VP
<input type="checkbox"/>	FG Private Subnet	eni-08adedc167a1180a6	subnet-0936fd8c6f4984efe	vpc-
<input checked="" type="checkbox"/>	FG Public Subnet	eni-03b2e198495d21f54	subnet-06ed7507849737ecf	vpc-

Network interface: eni-03b2e198495d21f54 (FG Public Subnet)

Details

Flow logs

Tags

You can now check network connectivity with Reachability Analyzer.

Network interface details

Actions

Create network interface

Attach

Detach

Delete

Manage IP addresses

Associate address

Disassociate address

Change termination behavior

Change security groups

Change source/dest. check

Manage tags

Manage prefixes

Change description

Create flow log

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

Change source/destination check

Network interface

eni-03b2e198495d21f54

Source/destination check

☐ Enable

Cancel

Save

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

9. Edit private route table.

Route tables (1/2) Info

Filter route tables

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
<input type="checkbox"/>	Public Route	rtb-0121768a9204bc14a	subnet-06ed750784973...	-	No	vpc-060a1e2007366fbf4 AW.
<input checked="" type="checkbox"/>	Private Route	rtb-087e78e7f2a174a94	-	-	Yes	vpc-060a1e2007366fbf4 AW.

rtb-087e78e7f2a174a94 / Private Route

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

Filter routes

Both

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Figure 10.143: Edit Private Route

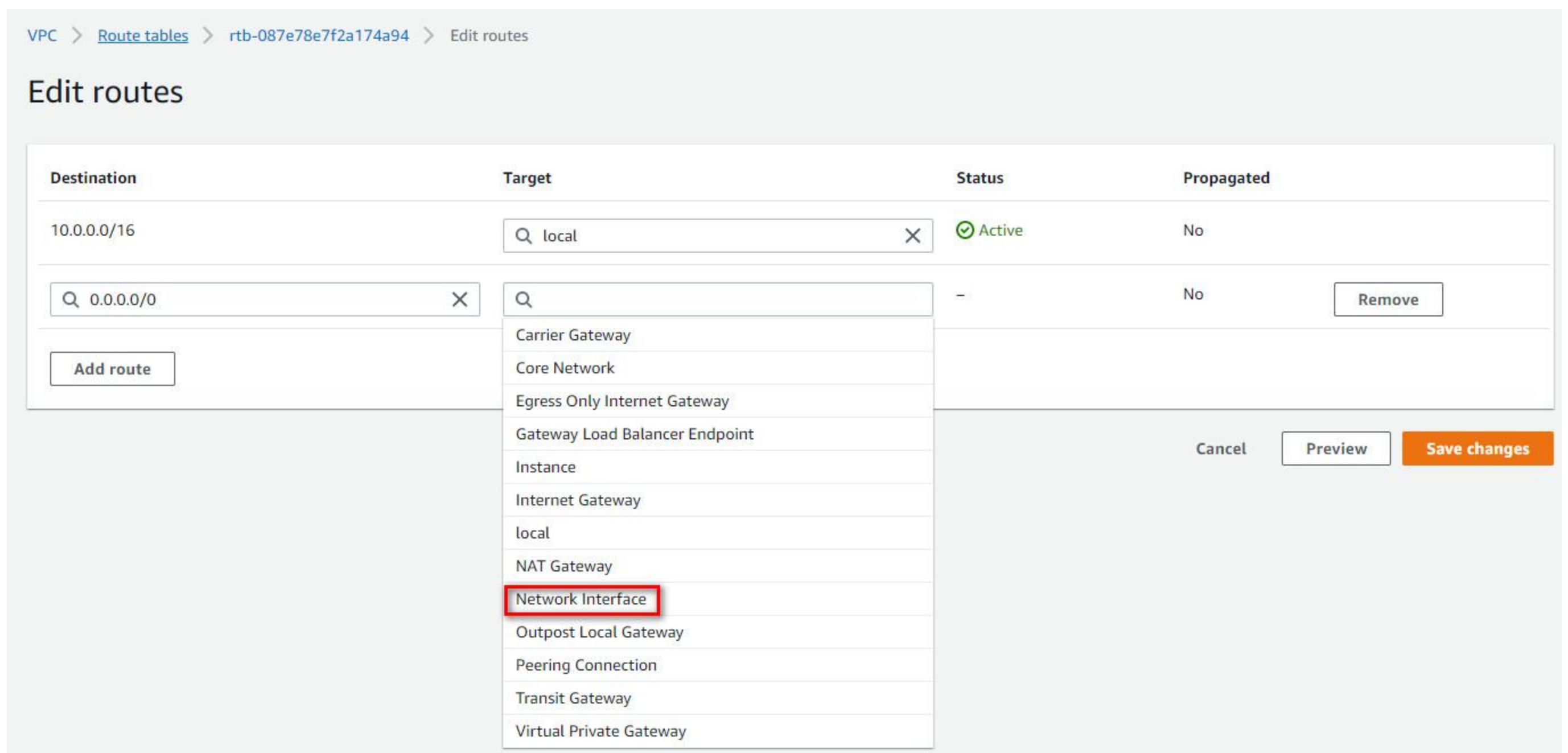


Figure 10.144: Add a default route and select Network Interface

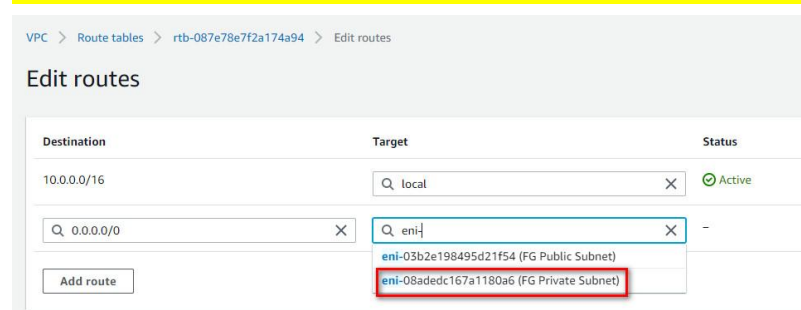


Figure 10.145: Add a default route to target FG Private Subnet

10. Verify Public and Private IP address of FG.

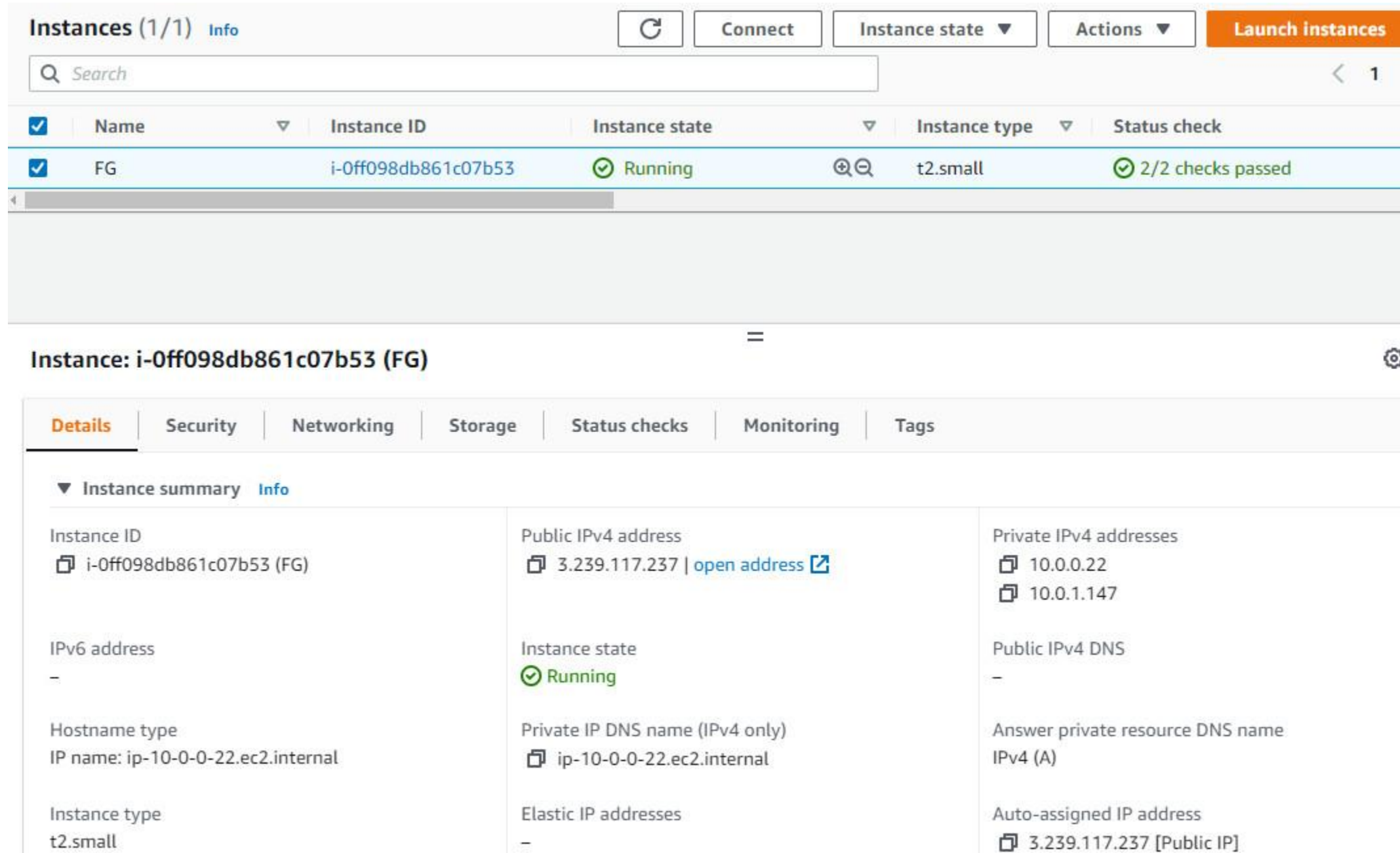


Figure 10.146: Verify public and private IP address of FG

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.

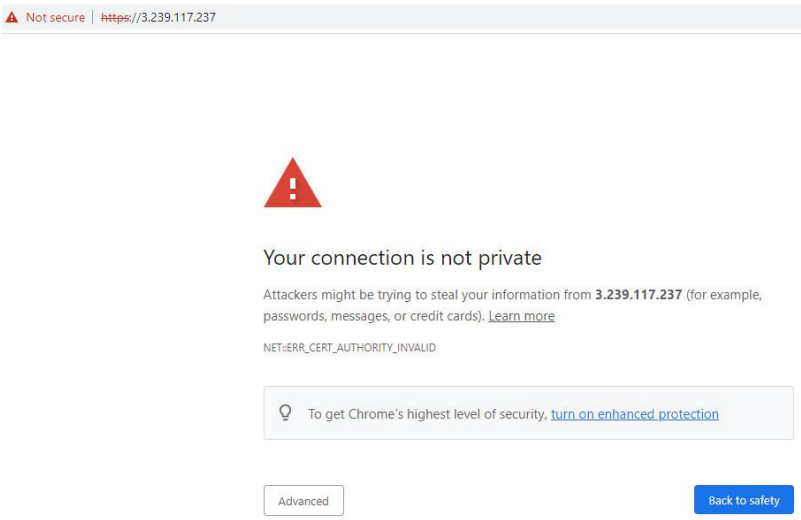


Figure 10.147: Access FortiGate

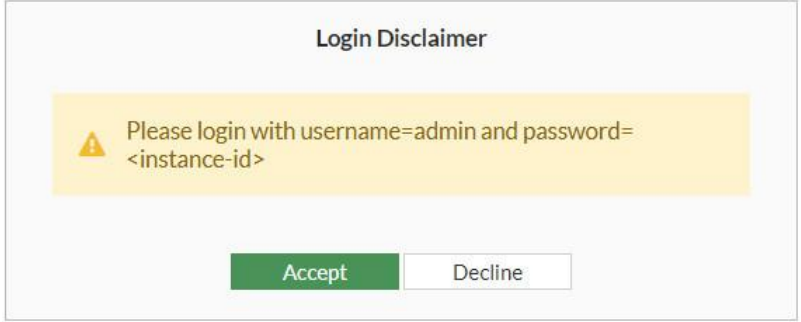


Figure 10.148: Access FortiGate

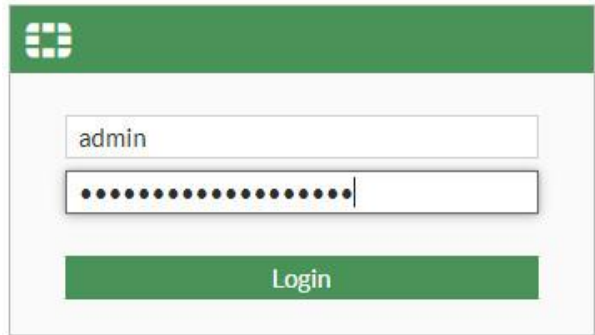


Figure 10.149: Username is admin and password is instance ID of FortiGate

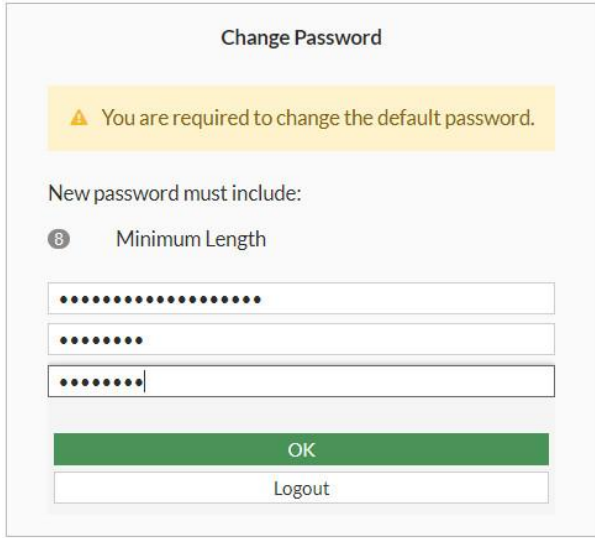


Figure 10.150: Change password

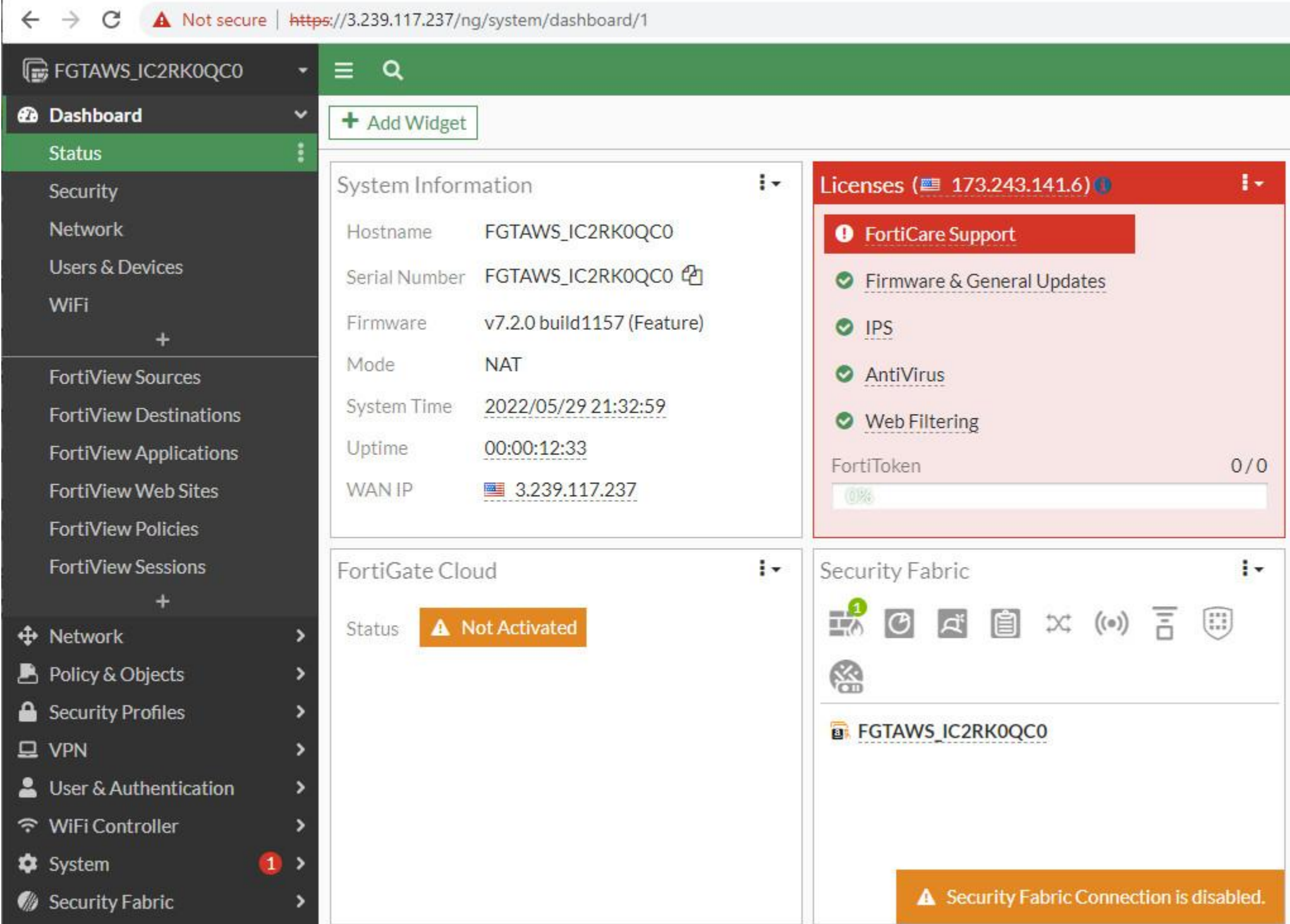


Figure 10.151: FortiGate dashboard

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.

Edit Interface

Name

port2

Alias

Type

Physical Interface

VRF ID

0

Role

Undefined

Dedicated Management Port

Address

Addressing mode

ManualDHCPAuto-managed by IPAMOne-Arm Sniffer

Retrieve default gateway from server

Distance

5

Override internal DNS

Administrative Access

IPv4

HTTPS

FMG-Access

FTM

Speed Test

HTTP

SSH

RADIUS Accounting

PING

SNMP

Security Fabric Connection

Receive LLDP

Use VDOM SettingEnableDisable

Figure 10.152: Change port2 to DHCP Client

FortiGate VM64-AWS

Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
Physical Interface				
port1	Physical Interface		10.0.0.22/255.255.255.0	PING HTTPS SSH HTTP FMG-Access
port2	Physical Interface		10.0.1.147/255.255.255.0	
Tunnel Interface				
NAT Interface (naf.root)		Tunnel Interface	0.0.0.0/0.0.0.0	

Figure 10.153: FortiGate interfaces