VPC and Peering

It’s a five tier Architecture

Problem Statement:

You work for XYZ Corporation and based on the expansion requirements of your corporation you have been asked to create and set up a distinct Amazon VPC for the production and development team. You are expected to perform the following tasks for the respective VPCs.

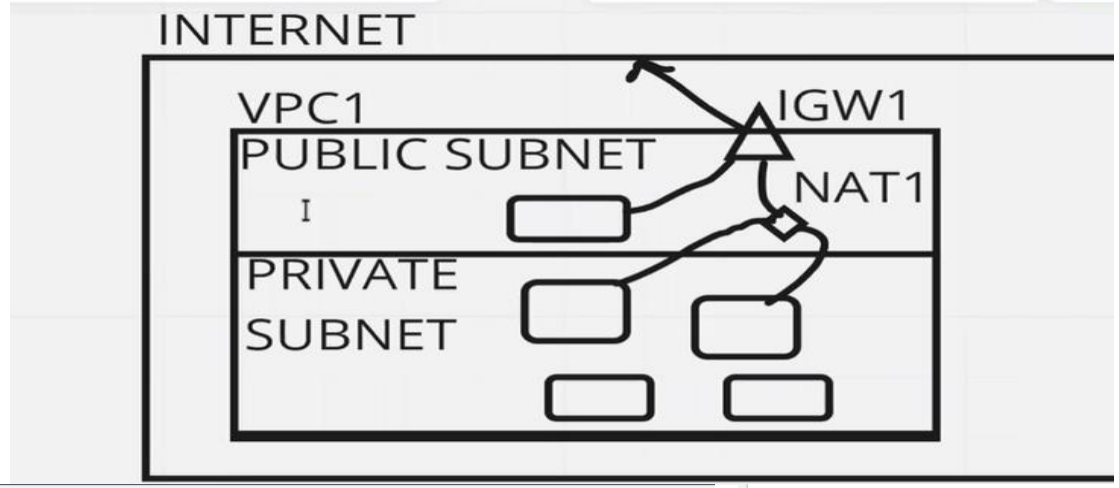
Production Network:

1. Design and build a 4-tier architecture.
2. Create 5 subnets out of which 4 should be private named app1, app2, dbcache and db and one should be public, named web.
3. Launch instances in all subnets and name them as per the subnet that they have been launched in.
4. Allow dbcache instance and app1 subnet to send internet requests.
5. Manage security groups and NACLs.

Development Network:

1. Design and build 2-tier architecture with two subnets named web and db and launch instances in both subnets and name them as per the subnet names.
2. Make sure only the web subnet can send internet requests.
3. Create peering connection between production network and development network.
4. Setup connection between db subnets of both production network and development network respectively.

Search for VPC service – go in vpc – choose create vpc.



VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

- (•) VPC only
- ( ) VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

vpc-1

IPv4 CIDR block Info

- (•) IPv4 CIDR manual input
- ( ) IPAM-allocated IPv4 CIDR block

IPv4 CIDR

11.11.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

- (•) No IPv6 CIDR block
- ( ) IPAM-allocated IPv6 CIDR block
- ( ) Amazon-provided IPv6 CIDR block
- ( ) IPv6 CIDR owned by me

IPv4 CIDR

11.11.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

- (•) No IPv6 CIDR block
- ( ) IPAM-allocated IPv6 CIDR block
- ( ) Amazon-provided IPv6 CIDR block
- ( ) IPv6 CIDR owned by me

Tenancy Info

Default

Tags

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.

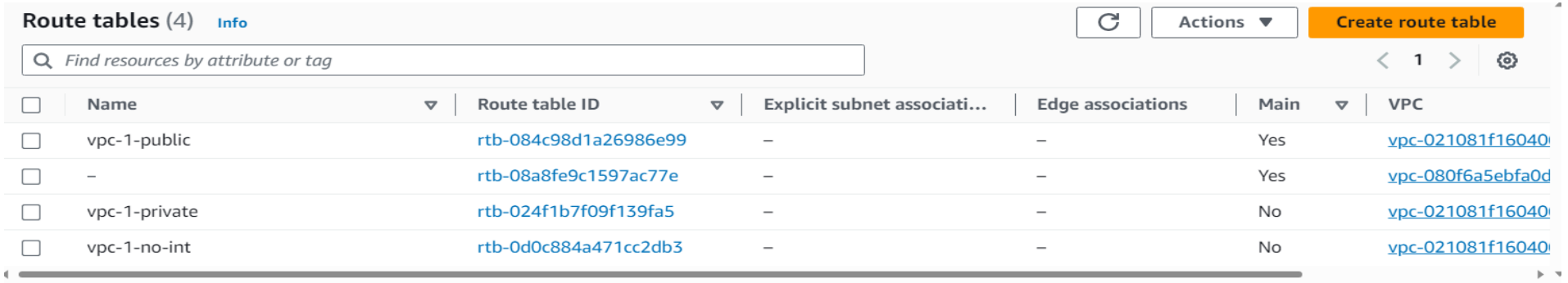
Key	Value - *optional*	
Name	vpc-1	Remove tag

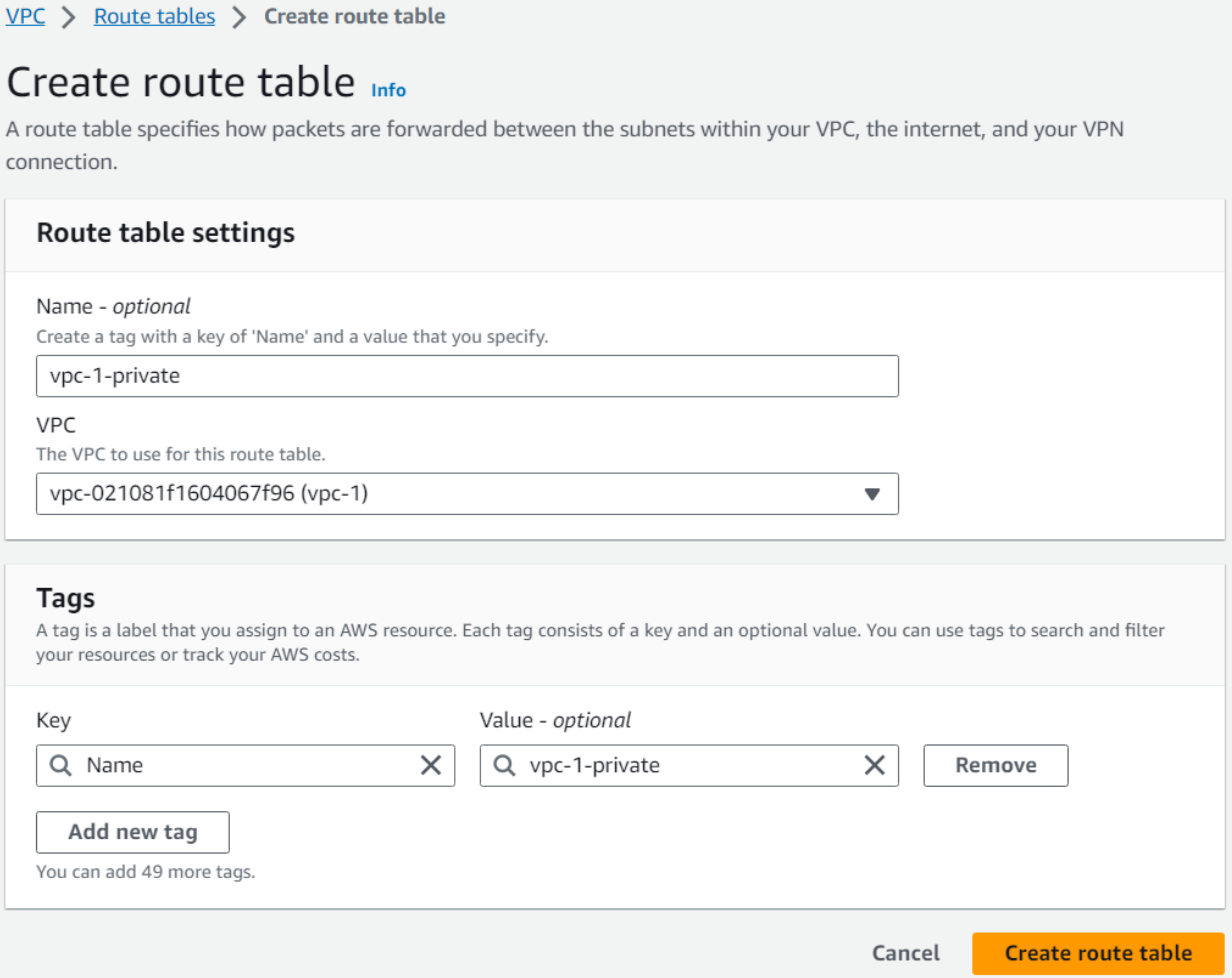
Add tag

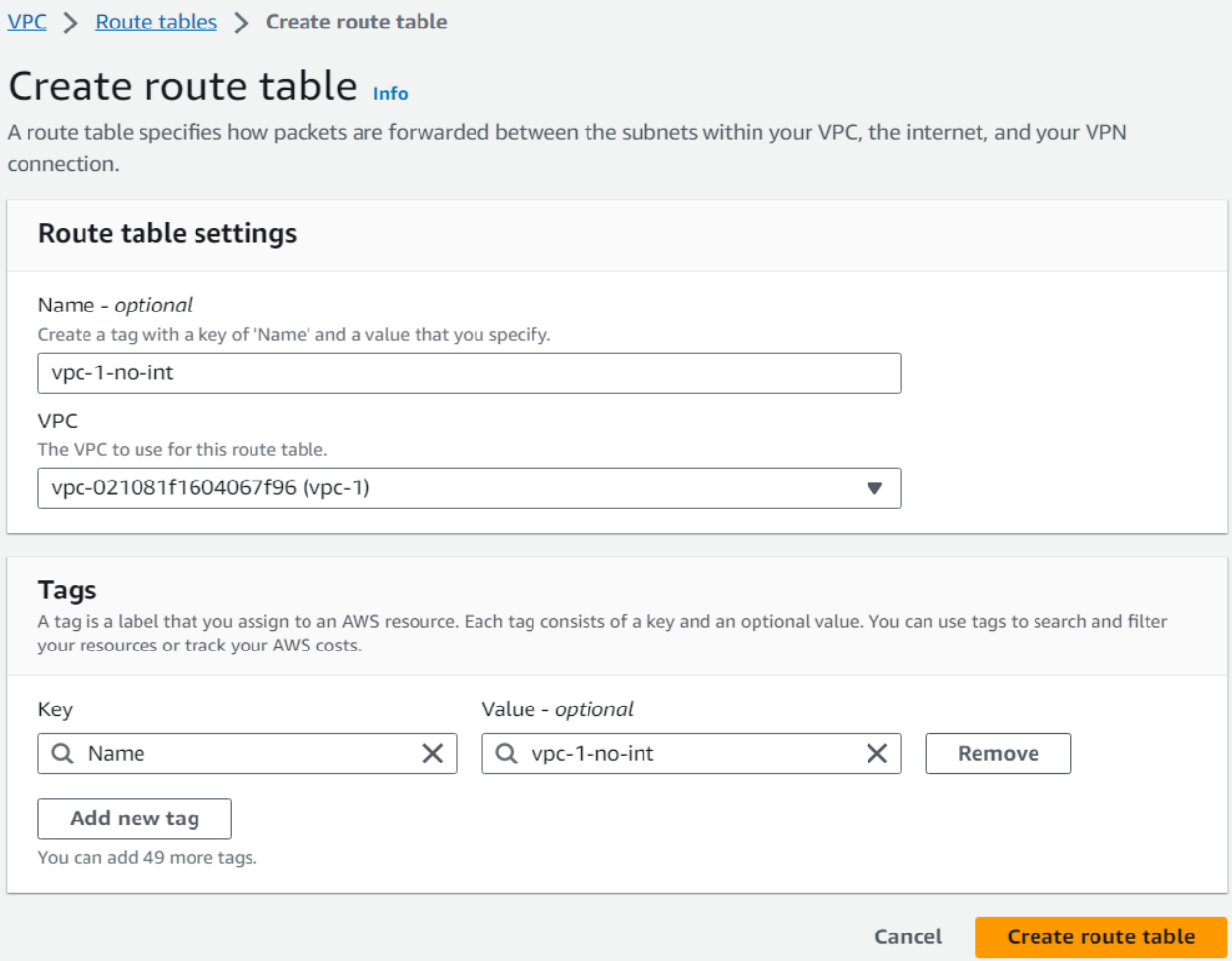
You can add 49 more tags

Cancel | Create VPC

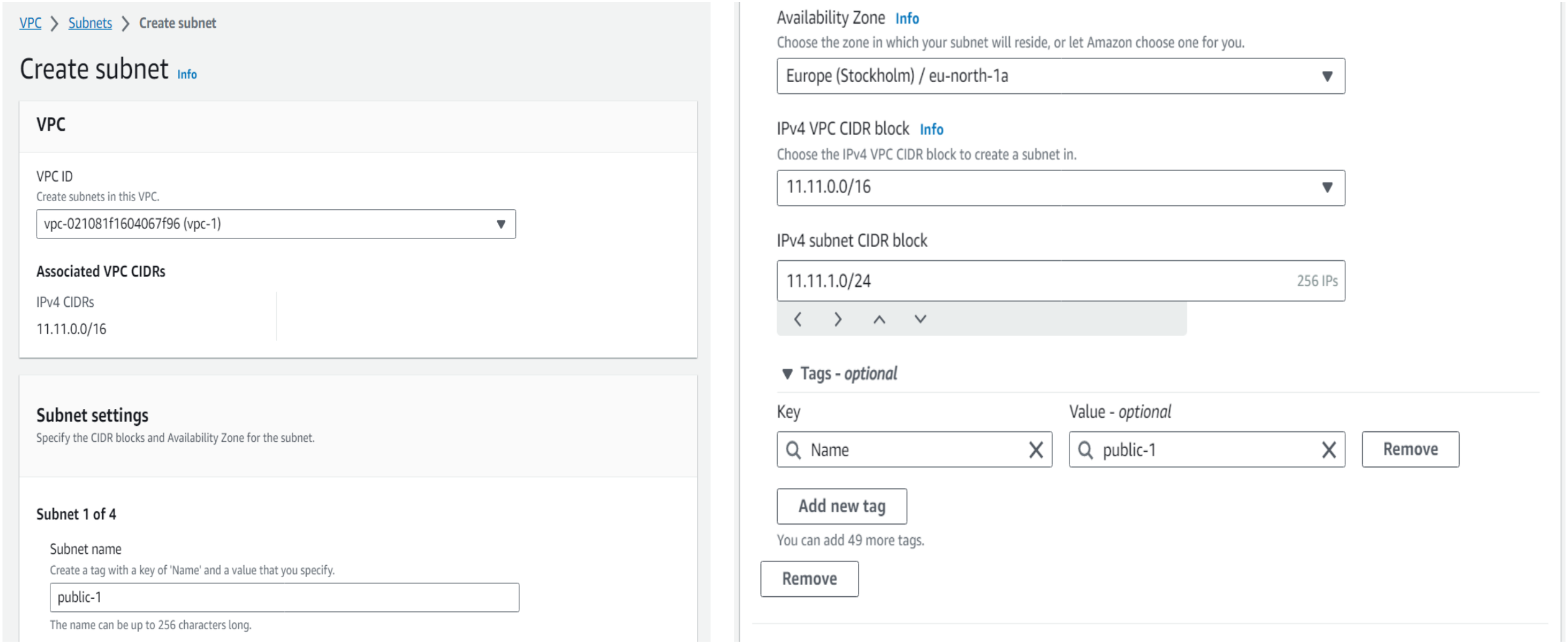
While creating the vpc the one route table is self create and we have to create two more route table.







Create four subnet public-1, private 1,2,3.



Subnet 2 of 4

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private-1
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.
Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block Info
Choose the IPv4 VPC CIDR block to create a subnet in.
11.11.0.0/16

IPv4 subnet CIDR block
11.11.2.0/24 256 IPs

Tags - *optional*

Key	Value - *optional*	
Name	private-1	Remove

Add new tag
You can add 49 more tags.

Remove

Subnet 3 of 4

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private-2
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.
Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block Info
Choose the IPv4 VPC CIDR block to create a subnet in.
11.11.0.0/16

IPv4 subnet CIDR block
11.11.3.0/24 256 IPs

Tags - *optional*

Key	Value - *optional*	
Name	private-2	Remove

Add new tag
You can add 49 more tags.

Remove

Subnet 4 of 4

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private-3
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.
Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block Info
Choose the IPv4 VPC CIDR block to create a subnet in.
11.11.0.0/16

IPv4 subnet CIDR block
11.11.4.0/24 256 IPs

Tags - *optional*

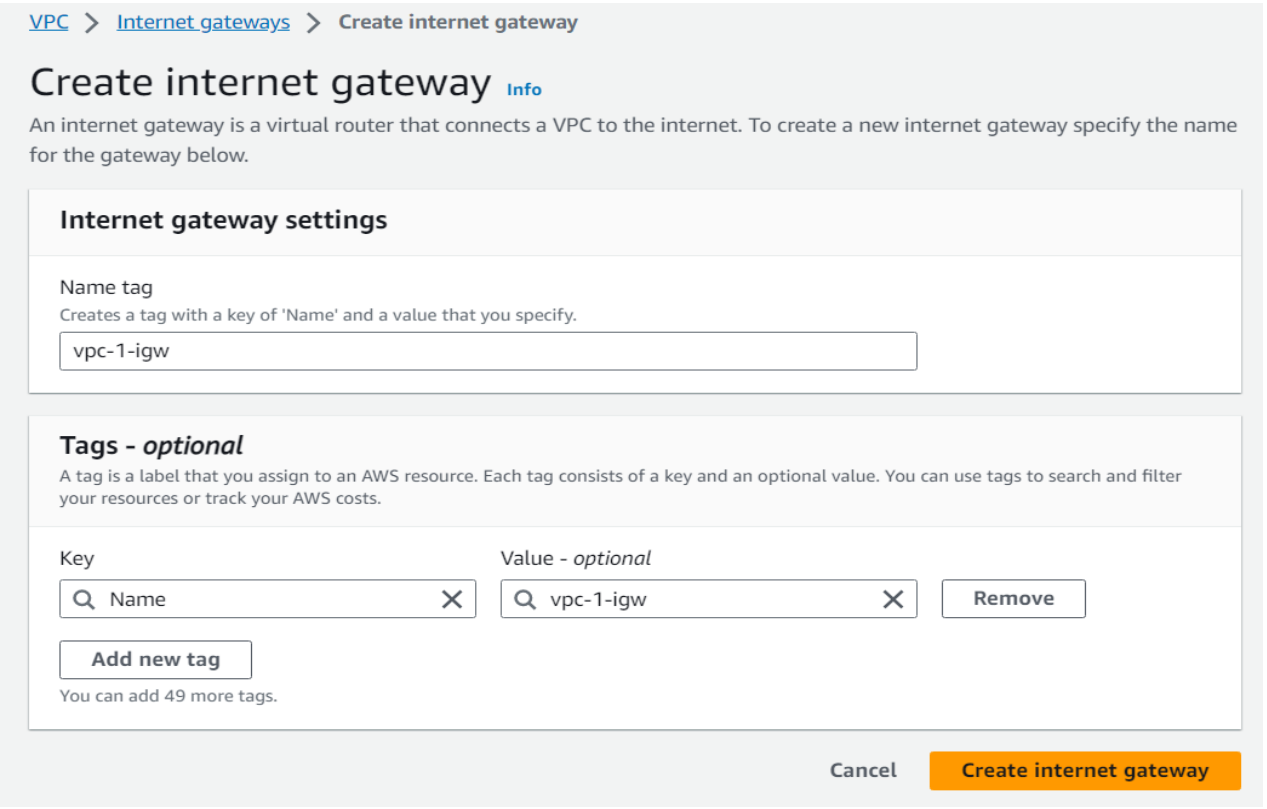
Key	Value - *optional*	
Name	private-3	Remove

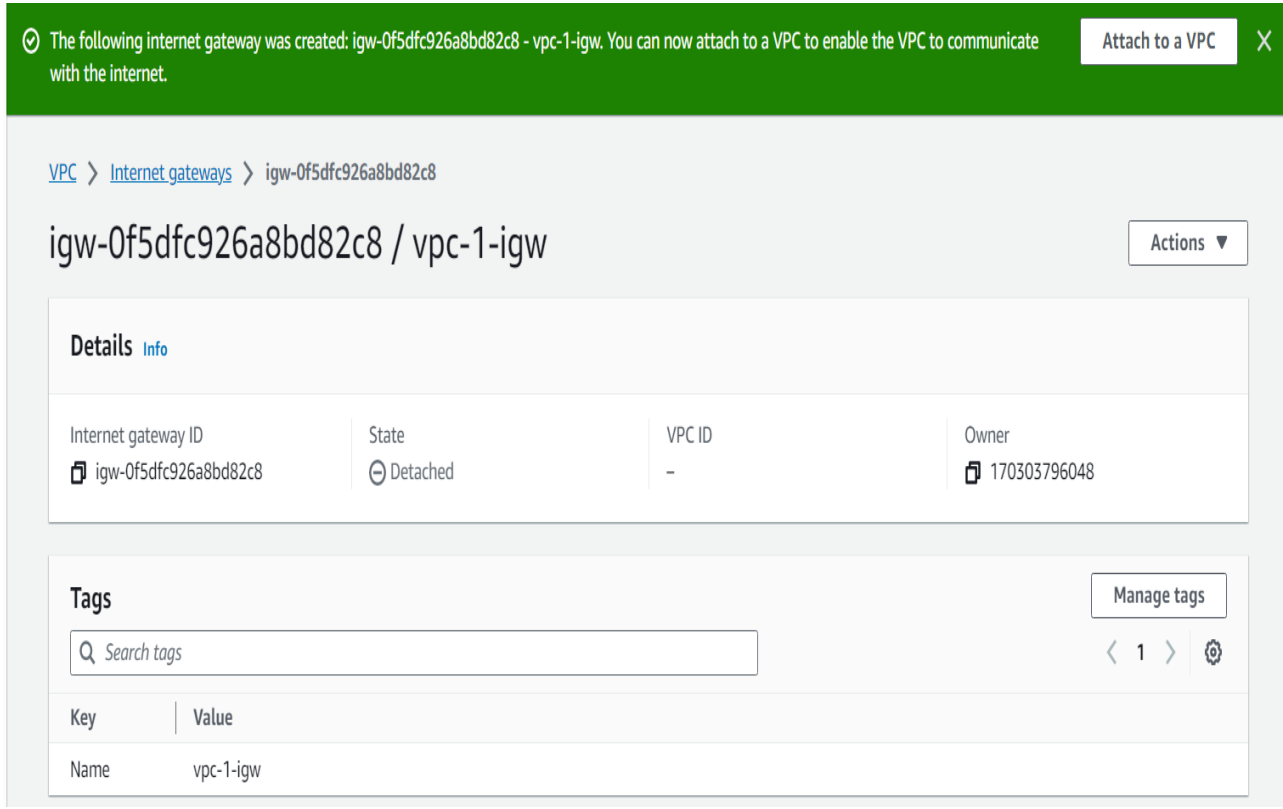
Add new tag
You can add 49 more tags.

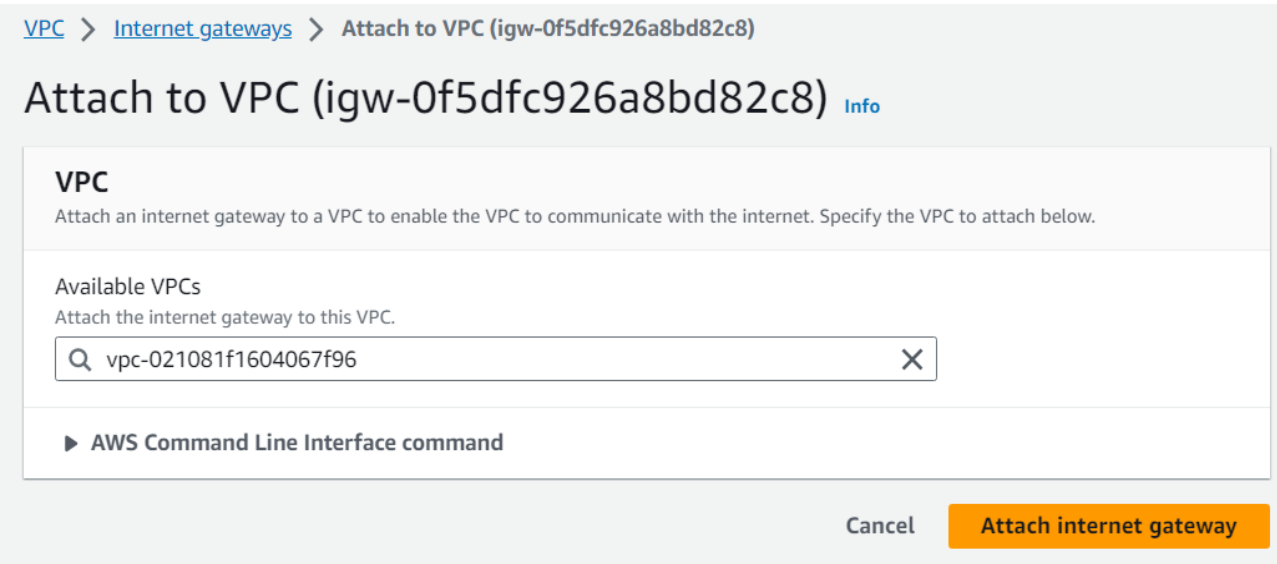
Remove

Name	Subnet ID	State	VPC	IPv4 CIDR
private-1	subnet-0d4294a4c225cb3bf	Available	vpc-021081f1604067f96 | vpc-1	11.11.2.0/24
private-2	subnet-0bb8367d00d8f2527	Available	vpc-021081f1604067f96 | vpc-1	11.11.3.0/24
private-3	subnet-0f52df4fa5788cddd	Available	vpc-021081f1604067f96 | vpc-1	11.11.4.0/24
public-1	subnet-0c6df3beb5f338064	Available	vpc-021081f1604067f96 | vpc-1	11.11.1.0/24

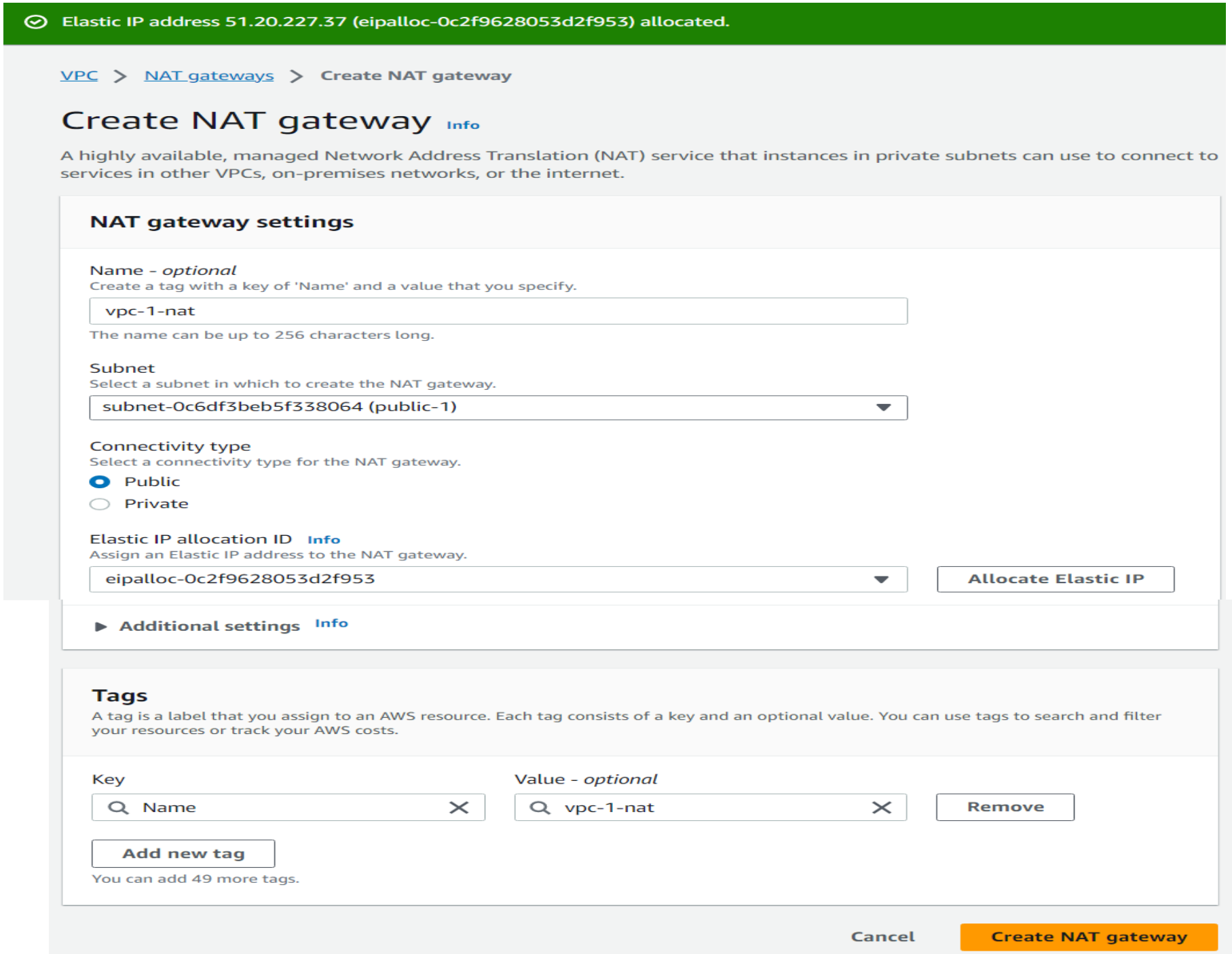
After creating the subnet we need to create internet gateway and attach to vpc.







After creating the IGW we need to create Nat gateway and allocate elastic IP.



VPC > Route tables > rtb-084c98d1a26986e99

rtb-084c98d1a26986e99 / vpc-1-public

Actions

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-084c98d1a26986e99	Yes	–	–

VPC	Owner ID
vpc-021081f1604067f96 | vpc-1	170303796048

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (1)

Both | Edit routes

Filter routes

1

Destination	Target	Status	Propagated
11.11.0.0/16	local	Active	No

Move in public route table – go on edit route – choose internet gateway – save changes.

Next associate subnet public one with same Route table.

VPC > Route tables > rtb-084c98d1a26986e99 > Edit routes

Edit routes

Destination	Target	Status	Propagated	
11.11.0.0/16	local local	Active	No	
0.0.0.0/0	Internet Gateway igw-	–	No	Remove

Add route

Cancel | Preview | Save changes

Routes | Subnet associations | Edge associations | Route propagation | Tags

Explicit subnet associations (1)

Find subnet association

Name	Subnet ID	IPv4 CIDR
public-1	subnet-0c6df3beb5f338064	11.11.1.0/24

Again do the same with Private-1 route table – edit route and associate subnet .

VPC > Route tables > rtb-024f1b7f09f139fa5 > Edit routes

Edit routes

Destination	Target	Status	Propagated	
11.11.0.0/16	local local	Active	No	
0.0.0.0/0	NAT Gateway nat-0253953185406f5e6	–	No	Remove

Add route

Cancel | Preview | Save changes

VPC > Route tables > rtb-024f1b7f09f139fa5 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

Filter subnet associations

1

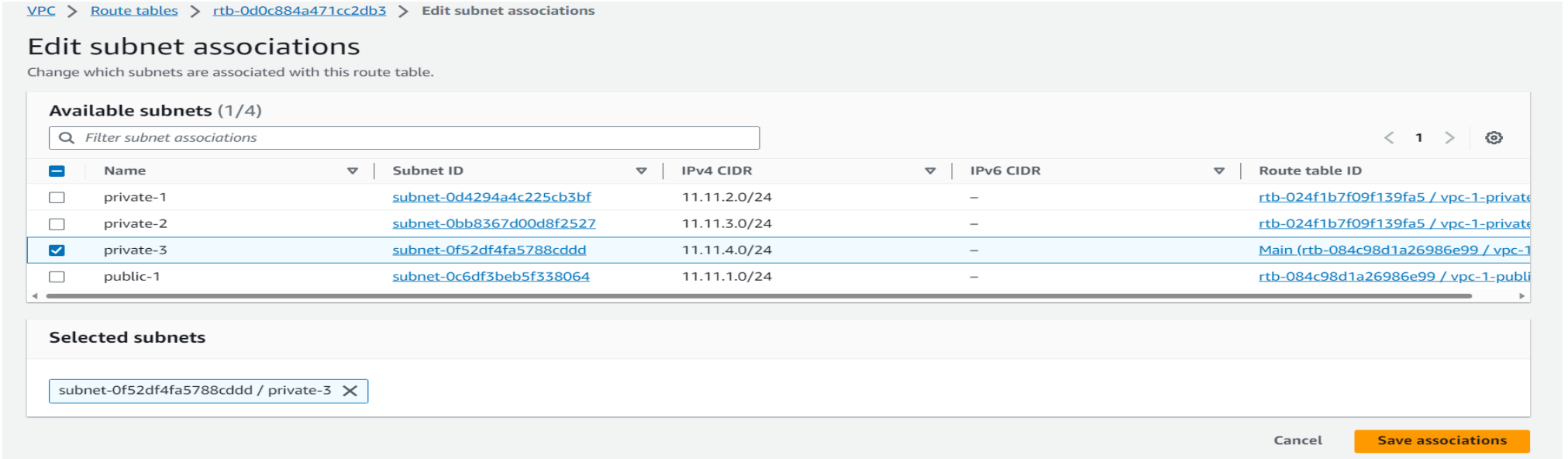
	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	private-1	subnet-0d4294a4c225cb3bf	11.11.2.0/24	–	Main (rtb-084c98d1a26986e99 / vpc-1
☑	private-2	subnet-0bb8367d00d8f2527	11.11.3.0/24	–	Main (rtb-084c98d1a26986e99 / vpc-1
☐	private-3	subnet-0f52df4fa5788cddd	11.11.4.0/24	–	Main (rtb-084c98d1a26986e99 / vpc-1
☐	public-1	subnet-0c6df3beb5f338064	11.11.1.0/24	–	rtb-084c98d1a26986e99 / vpc-1-publi

Selected subnets

subnet-0d4294a4c225cb3bf / private-1 | subnet-0bb8367d00d8f2527 / private-2

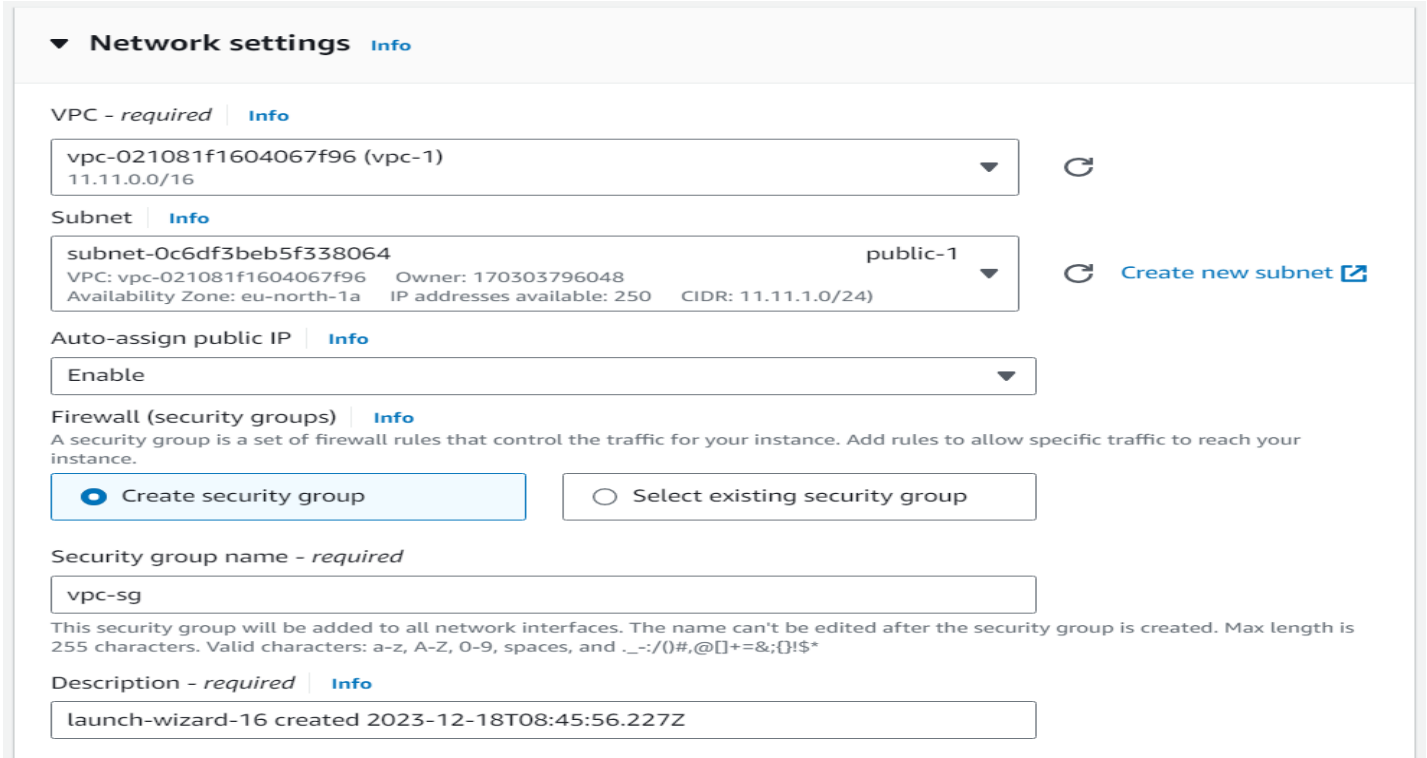
Cancel | Save associations

As with no internet route table we don’t need to edit route because it doesn’t have internet connectivity, only associate subnet .

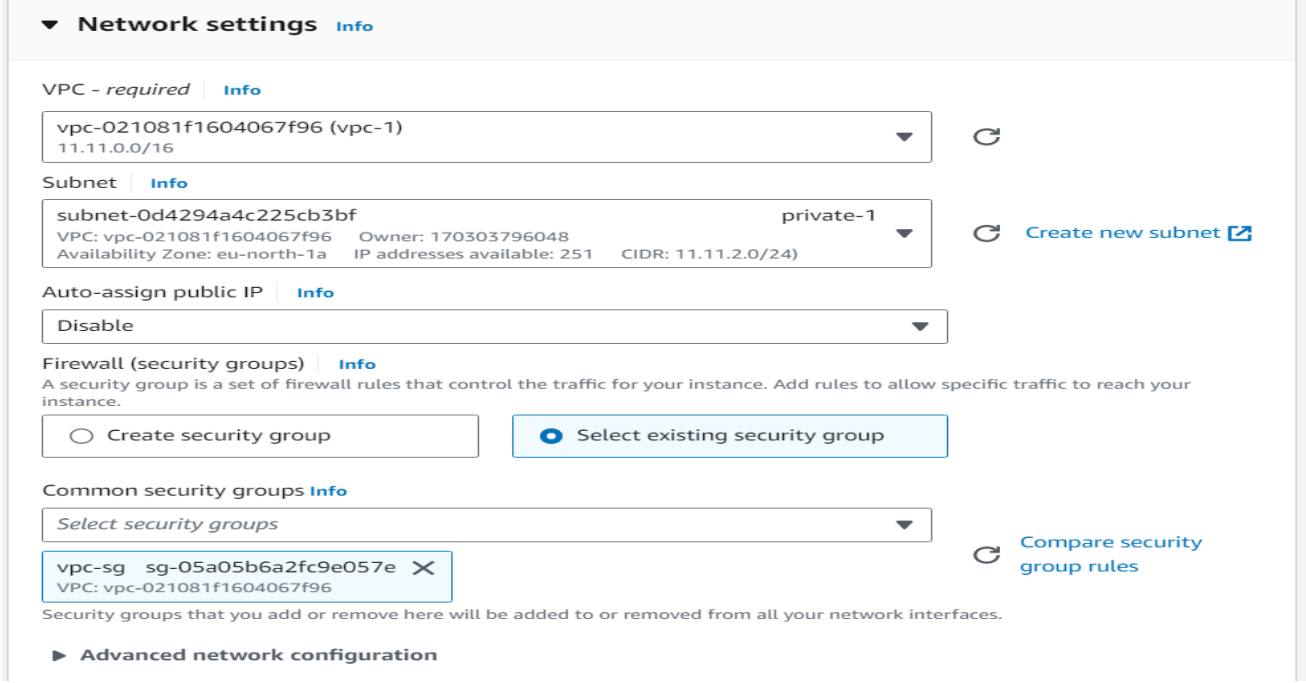


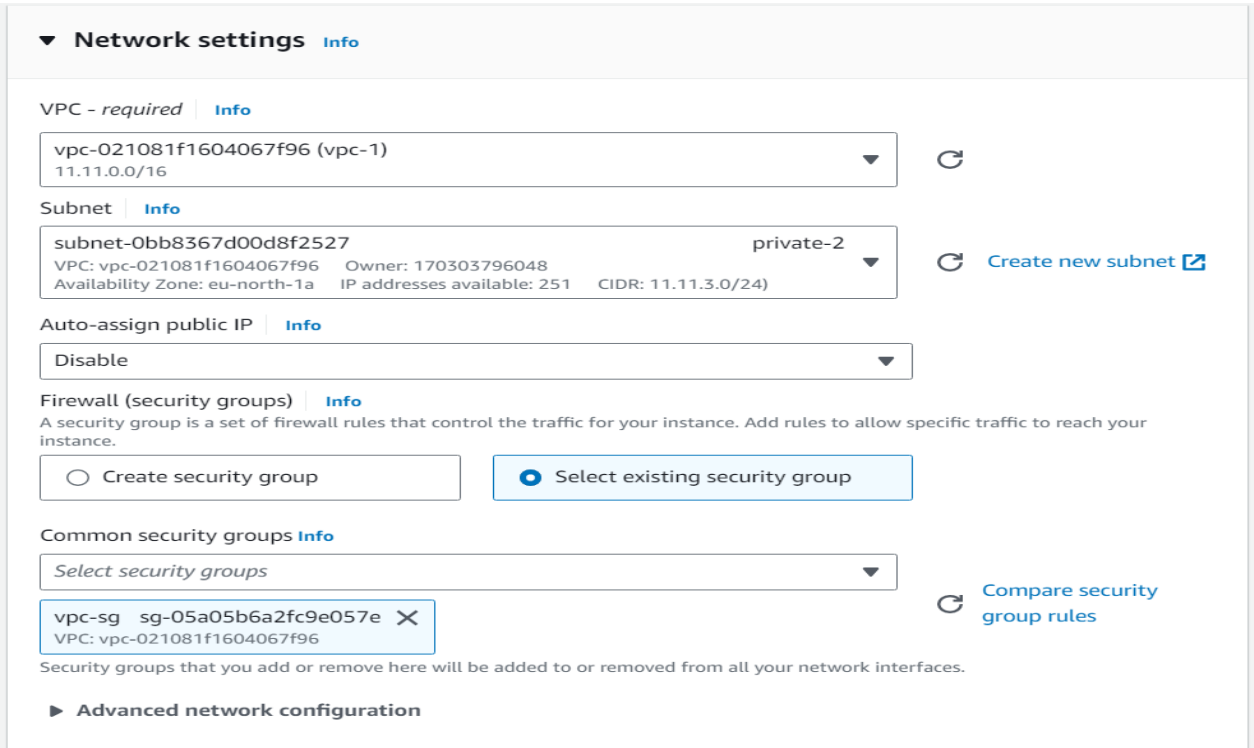
Now we are going to launch instances in each public subnets using vpc-1.

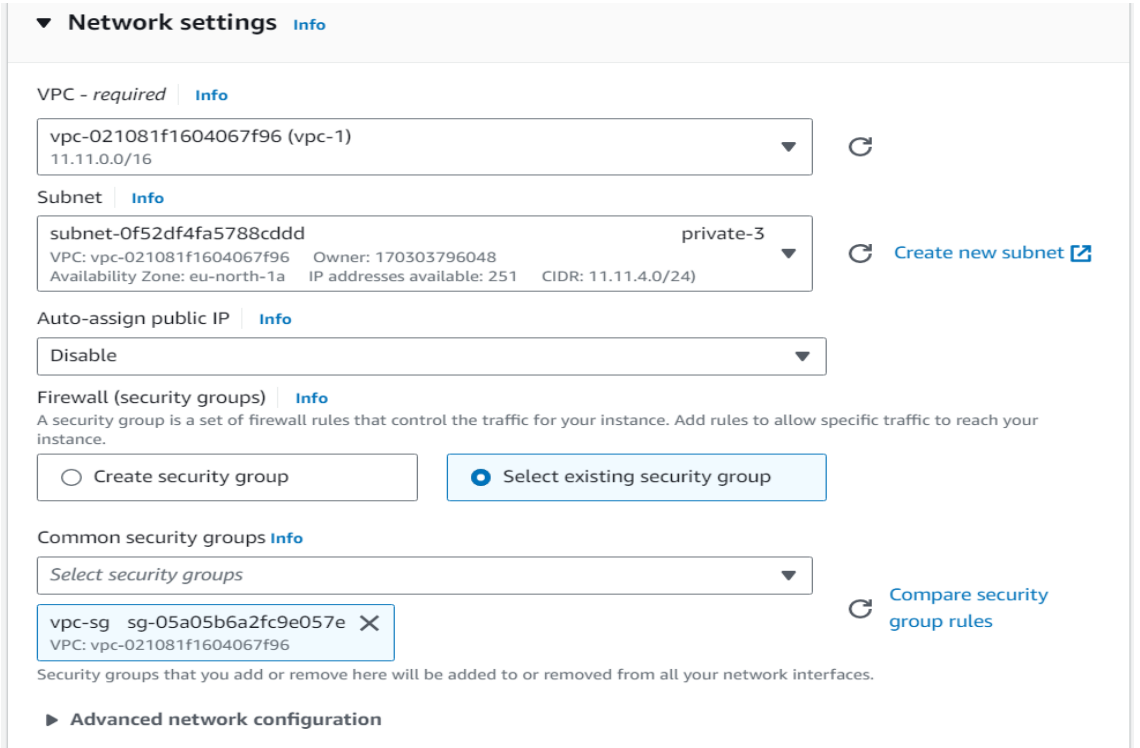
Launch instance one in public subnet , vpc-1 with elastic ip enable and security group with all traffic allowed .



Auto assign public ip is disable in private subnet instances.







Instances (4) Info

Connect | Instance state | Actions | Launch instances

Find Instance by attribute or tag (case-sensitive)

1

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Pub
public-1	i-0394f268fc44178cb	Running	t3.micro	2/2 checks passed	No alarms	eu-north-1a	–
private-1	i-0105d0988b6915c6a	Running	t3.micro	2/2 checks passed	No alarms	eu-north-1a	–
private-2	i-09b3f63f61b71bd75	Running	t3.micro	2/2 checks passed	No alarms	eu-north-1a	–
private-3	i-04fdb157d95daeffa	Running	t3.micro	2/2 checks passed	No alarms	eu-north-1a	–

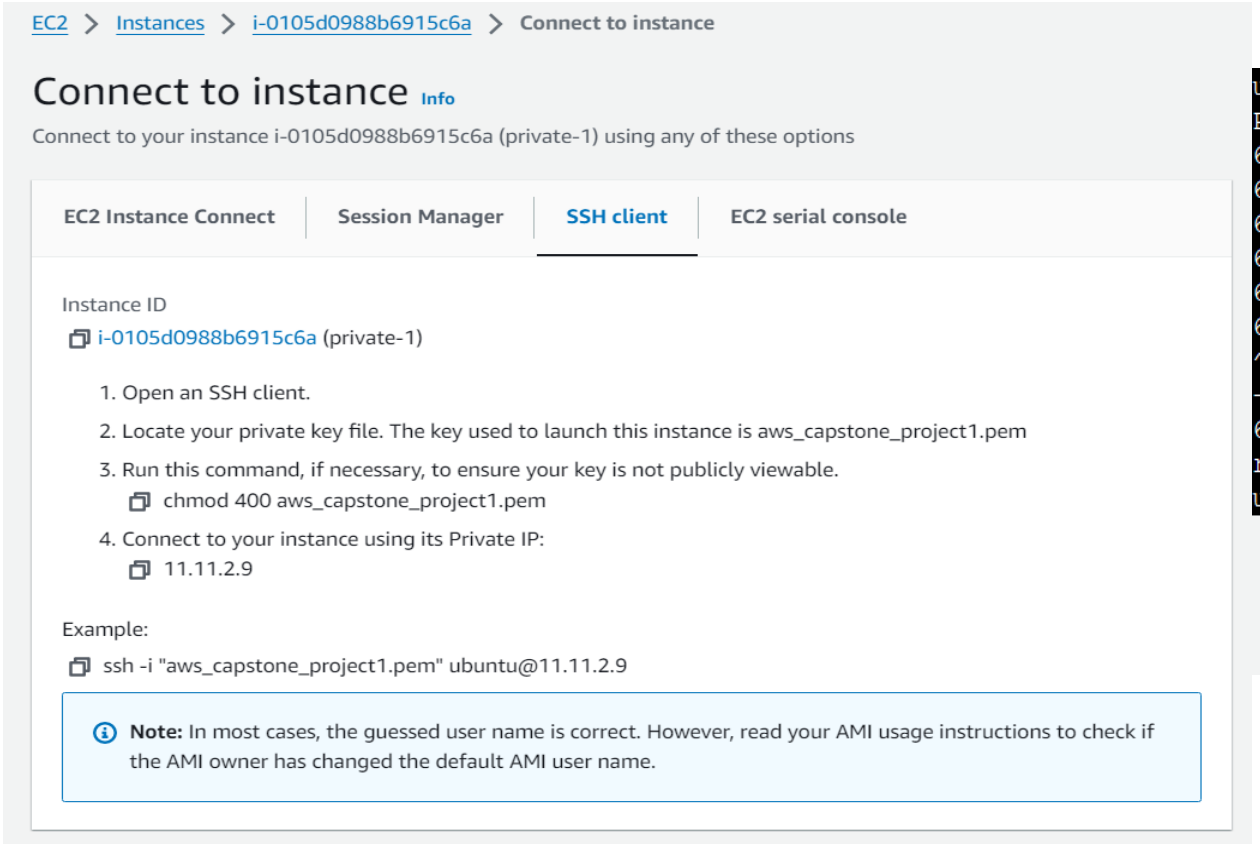
Connect to machine one check it has internet connectivity.

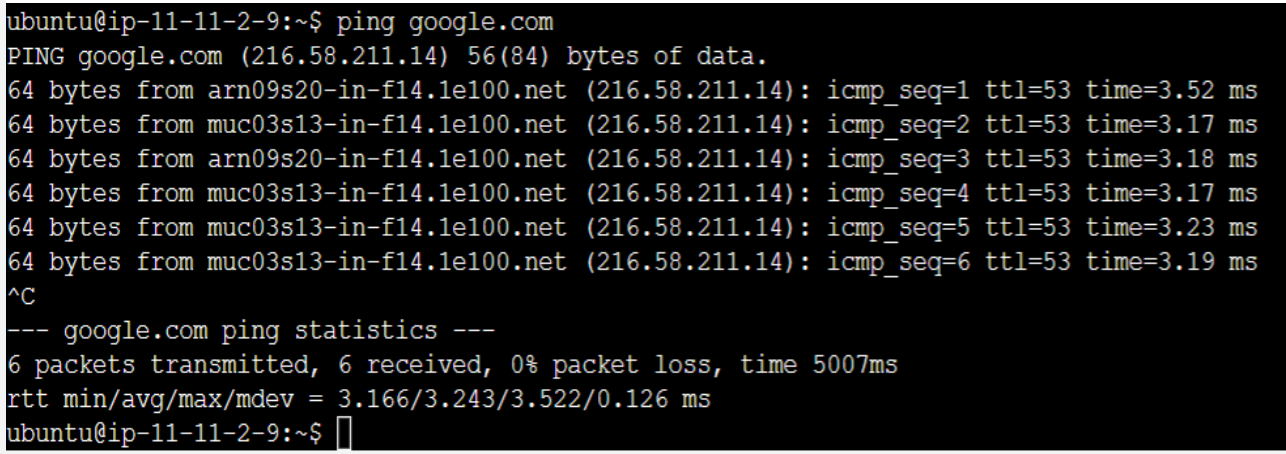
```
ubuntu@ip-11-11-1-234:~$ ping google.com
PING google.com (142.250.74.142) 56(84) bytes of data.
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=1 ttl=114 time=3.44 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=2 ttl=114 time=3.47 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=3 ttl=114 time=3.46 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=4 ttl=114 time=3.49 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=5 ttl=114 time=3.47 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=6 ttl=114 time=3.49 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 3.442/3.471/3.493/0.016 ms
ubuntu@ip-11-11-1-234:~$
```

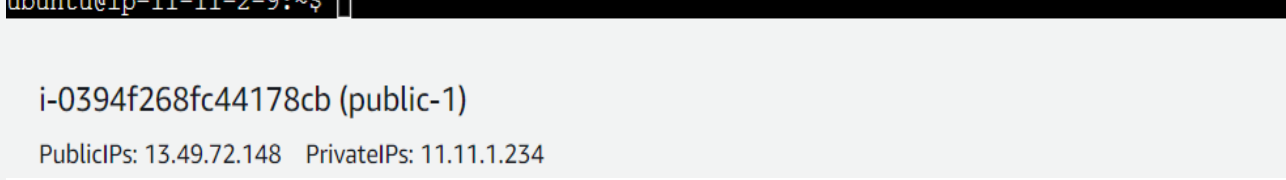
i-0394f268fc44178cb (public-1)

PublicIPs: 13.49.72.148 PrivateIPs: 11.11.1.234

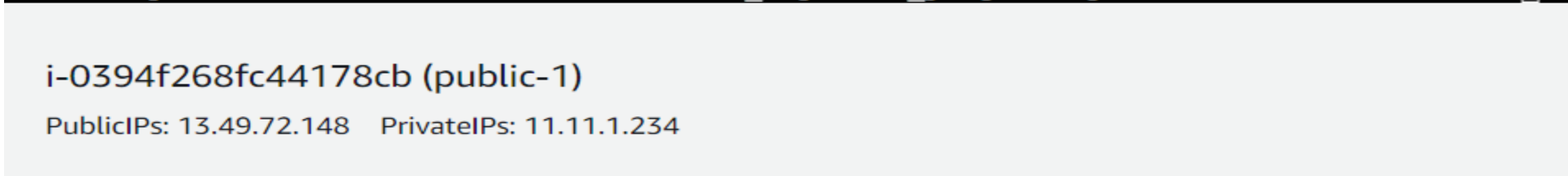
We cannot connect to private subnet instances directly so we can connect through SSH connection using the .pem key pair.
For connecting the private 1 instance – go in public-1 instance – create a nano file aws_capstone_project1.pem paste the key inside the file then paste sudo chmod command and at last ssh-i----------2.9 command and connect .







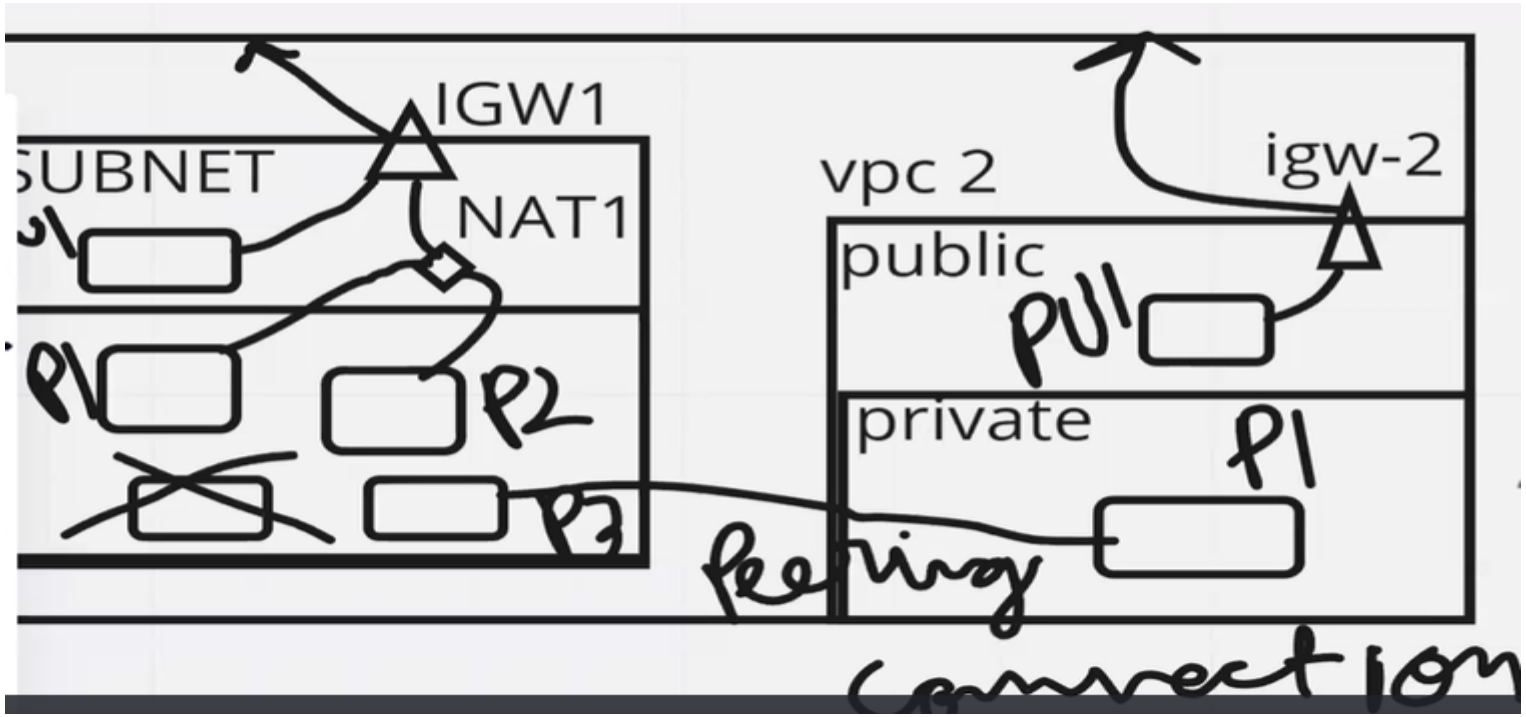
This time for connecting the private-2 machine we don't need to create nano file and paste chmod command .



```
ubuntu@ip-11-11-3-240:~$ ping google.com
PING google.com (142.250.74.142) 56(84) bytes of data.
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=1 ttl=112 time=3.34 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=2 ttl=112 time=3.02 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=3 ttl=112 time=2.96 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=4 ttl=112 time=2.93 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=5 ttl=112 time=2.96 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.933/3.042/3.340/0.151 ms
ubuntu@ip-11-11-3-240:~$
```

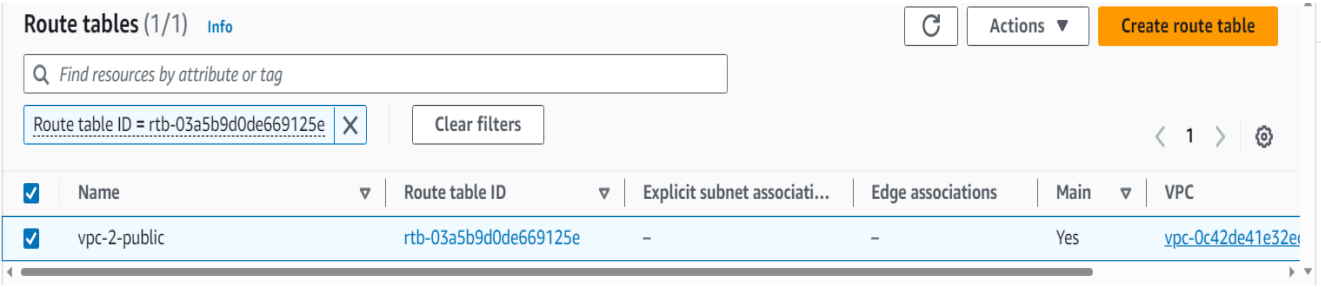
i-0394f268fc44178cb (public-1)

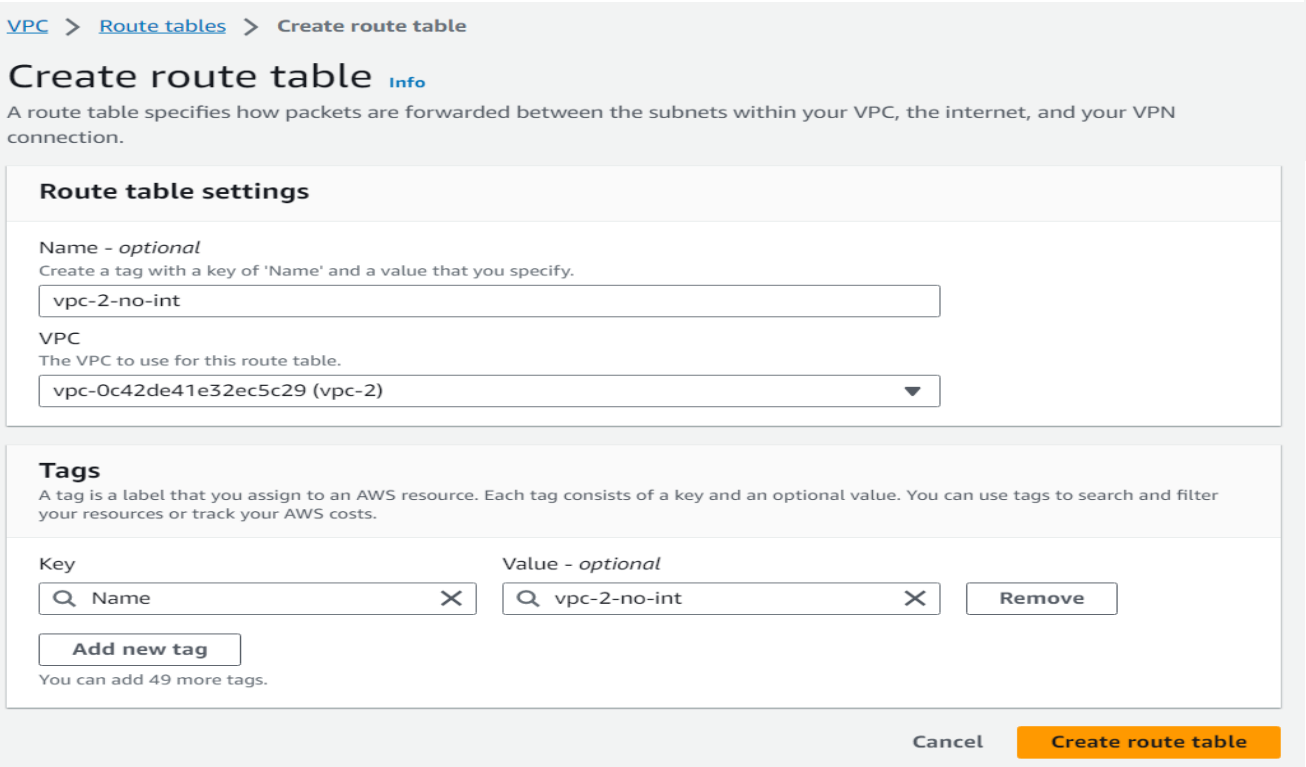
PublicIPs: 13.49.72.148 PrivateIPs: 11.11.1.234

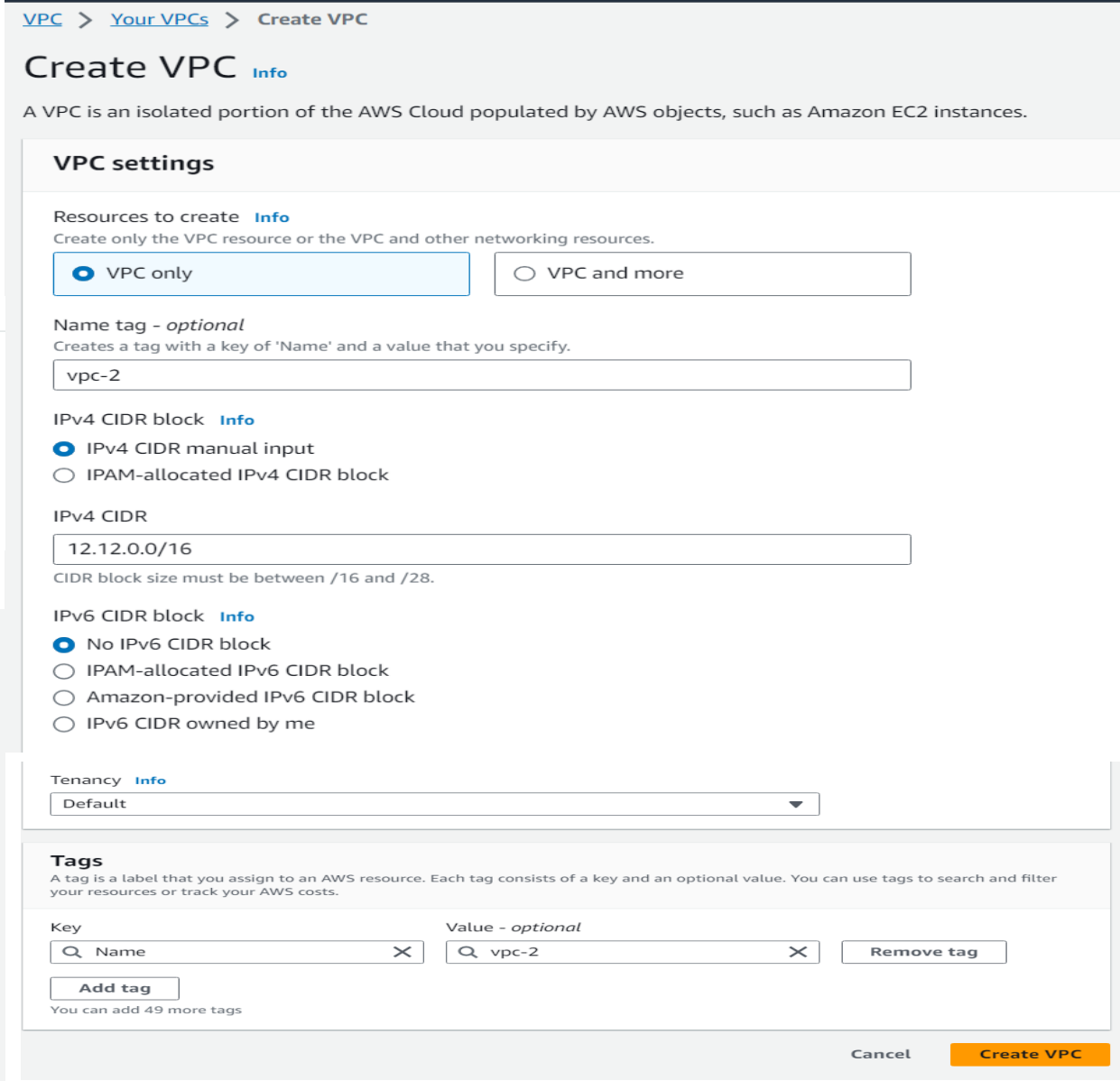


For development network we are going to follow the steps.

Name the Route table associated to this VPC.







We need to create one more route table with no internet.

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0c42de41e32ec5c29 (vpc-2)

Associated VPC CIDRs

IPv4 CIDRs
12.12.0.0/16

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
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.
Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block Info
Choose the IPv4 VPC CIDR block to create a subnet in.
12.12.0.0/16

IPv4 subnet CIDR block
12.12.1.0/24 256 IPs

▼ Tags - *optional*

Key: Name
Value - *optional*: public
Remove

Add new tag
You can add 49 more tags.

Remove

The next step is to create subnets.

Subnet 2 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private
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.
Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block Info
Choose the IPv4 VPC CIDR block to create a subnet in.
12.12.0.0/16

IPv4 subnet CIDR block
12.12.2.0/24 256 IPs

▼ Tags - *optional*

Key: Name
Value - *optional*: private
Remove

Add new tag
You can add 49 more tags.

Remove

Add new subnet

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
Creates a tag with a key of 'Name' and a value that you specify.
vpc-2-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	vpc-2-igw	Remove

Add new tag
You can add 49 more tags.

Cancel | Create internet gateway

The following internet gateway was created: igw-03ddd04d530b1b245 - vpc-2-igw. You can now attach to a VPC to enable the VPC to communicate with the internet. Attach to a VPC

VPC > Internet gateways > igw-03ddd04d530b1b245

igw-03ddd04d530b1b245 / vpc-2-igw

Actions

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-03ddd04d530b1b245	Detached	–	170303796048

Tags

Manage tags

Search tags

Key	Value
Name	vpc-2-igw

In VPC-2-PUBLIC Route table edit route attach to igw-2.

VPC > Route tables > rtb-03a5b9d0de669125e > Edit routes

Edit routes

Destination	Target	Status	Propagated	
12.12.0.0/16	local / local	Active	No	
0.0.0.0/0	Internet Gateway / igw-03ddd04d530b1b245	–	No	Remove

Add route

Cancel | Preview | Save changes

VPC > Internet gateways > Attach to VPC (igw-03ddd04d530b1b245)

Attach to VPC (igw-03ddd04d530b1b245) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.
vpc-0c42de41e32ec5c29

▶ AWS Command Line Interface command

Cancel | Attach internet gateway

In subnet association choose public subnet .

Routes | Subnet associations | Edge associations | Route propagation | Tags

Explicit subnet associations (1)

Find subnet association

Name	Subnet ID	IPv4 CIDR
public	subnet-00086a540dae32f1c	12.12.1.0/24

In vpc-2-no-int Route table edit subnet association and private subnet.

VPC > Route tables > rtb-0849efb04a0d6058b > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Filter subnet associations

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☐	public	subnet-00086a540dae32f1c	12.12.1.0/24	–	rtb-03a5b9d0de669125e / vpc-2-publi
☑	private	subnet-078f35e3e0a846876	12.12.2.0/24	–	Main (rtb-03a5b9d0de669125e / vpc-.

Selected subnets

subnet-078f35e3e0a846876 / private

Cancel | Save associations

Network settings Info

VPC - *required* Info

vpc-0c42de41e32ec5c29 (vpc-2)
12.12.0.0/16

Subnet Info

subnet-078f35e3e0a846876 private
VPC: vpc-0c42de41e32ec5c29 Owner: 170303796048
Availability Zone: eu-north-1a IP addresses available: 251 CIDR: 12.12.2.0/24)

Create new subnet

Auto-assign public IP Info

Disable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group ● Select existing security group

Common security groups Info

Select security groups

vpc-2-sg sg-00d3d4cd5aa17ec3f
VPC: vpc-0c42de41e32ec5c29

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▶ Advanced network configuration

Network settings Info

VPC - *required* Info

vpc-0c42de41e32ec5c29 (vpc-2)
12.12.0.0/16

Subnet Info

subnet-00086a540dae32f1c public
VPC: vpc-0c42de41e32ec5c29 Owner: 170303796048
Availability Zone: eu-north-1a IP addresses available: 251 CIDR: 12.12.1.0/24)

Create new subnet

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*

vpc-2-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

launch-wizard-16 created 2023-12-18T10:23:11.577Z

Inbound Security Group Rules

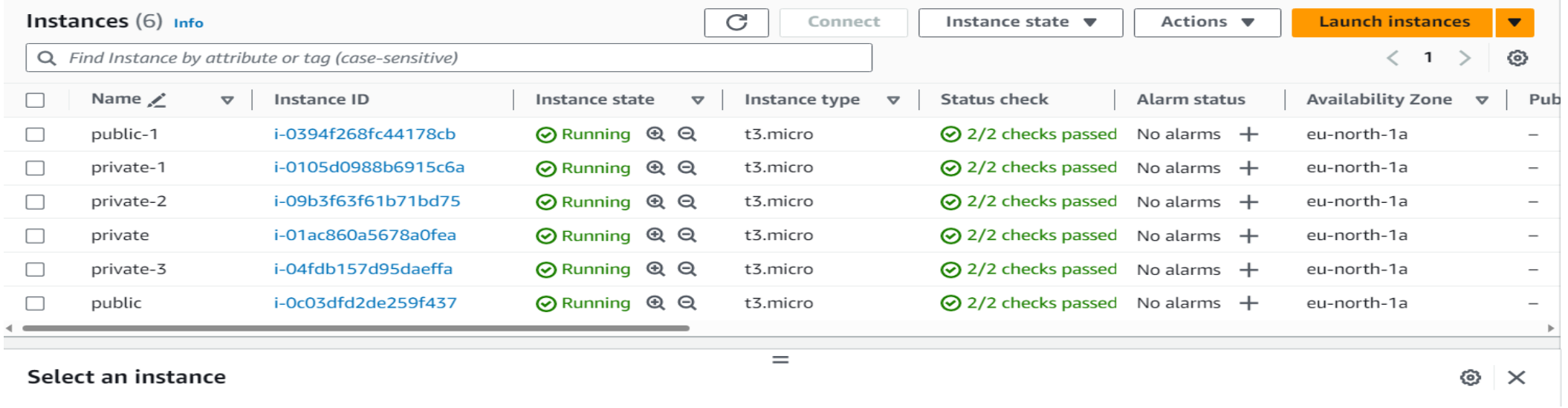
Security group rule 1 (All, All, 0.0.0.0/0) Remove

Type Info	Protocol Info	Port range Info
All traffic	All	All

Source type Info	Source Info	Description - *optional* Info
Anywhere	Add CIDR, prefix list or security	e.g. SSH for admin desktop

0.0.0.0/0

Launch two instances with these specifications.



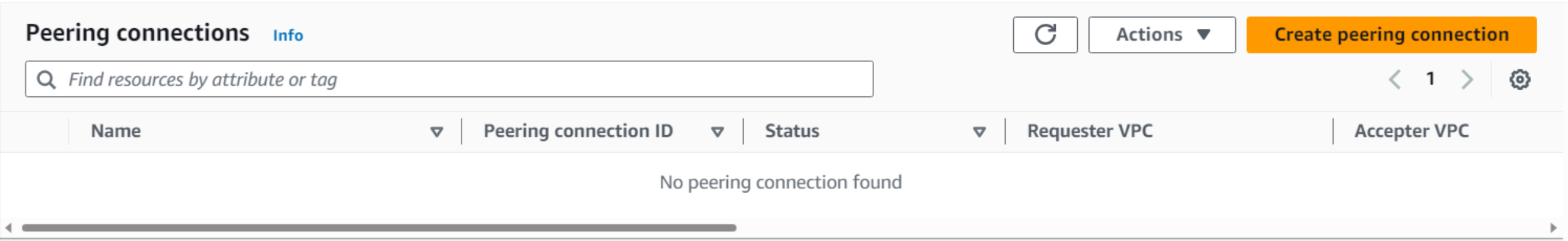
Let’s connect to the public instance which has vpc-2 connection and check the internet connectivity.

```
ubuntu@ip-12-12-1-124:~$ ping google.com
PING google.com (142.250.74.46) 56(84) bytes of data.
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=1 ttl=55 time=2.88 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=2 ttl=55 time=2.91 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=3 ttl=55 time=2.93 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=4 ttl=55 time=2.92 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=5 ttl=55 time=2.93 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=6 ttl=55 time=2.93 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=7 ttl=55 time=2.97 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=8 ttl=55 time=3.01 ms
^C
--- google.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 2.880/2.935/3.012/0.037 ms
ubuntu@ip-12-12-1-124:~$
```

i-0c03dfd2de259f437 (public)

PublicIPs: 13.53.93.143 PrivateIPs: 12.12.1.124

Now it’s time to create peering connection .



VPC > Peering connections > Create peering connection

Create peering connection

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Info

Peering connection settings

Name - *optional*

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

vpc1-vpc2-pc

Select a local VPC to peer with

VPC ID (Requester)

vpc-021081f1604067f96 (vpc-1)

VPC CIDRs for vpc-021081f1604067f96 (vpc-1)

CIDR	Status	Status reason
11.11.0.0/16	Associated	-

Select another VPC to peer with

Account

- (●) My account
- ( ) Another account

Region

- (●) This Region (eu-north-1)
- ( ) Another Region

VPC ID (Accepter)

vpc-0c42de41e32ec5c29 (vpc-2)

VPC CIDRs for vpc-0c42de41e32ec5c29 (vpc-2)

CIDR	Status	Status reason
12.12.0.0/16	Associated	-

Tags

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.

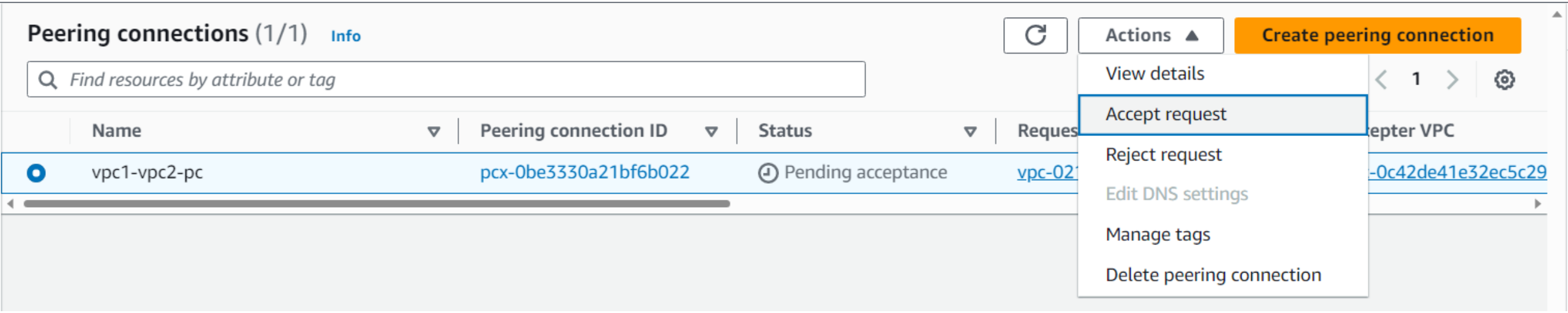
Key	Value - *optional*	
Name	vpc1-vpc2-pc	Remove

Add new tag

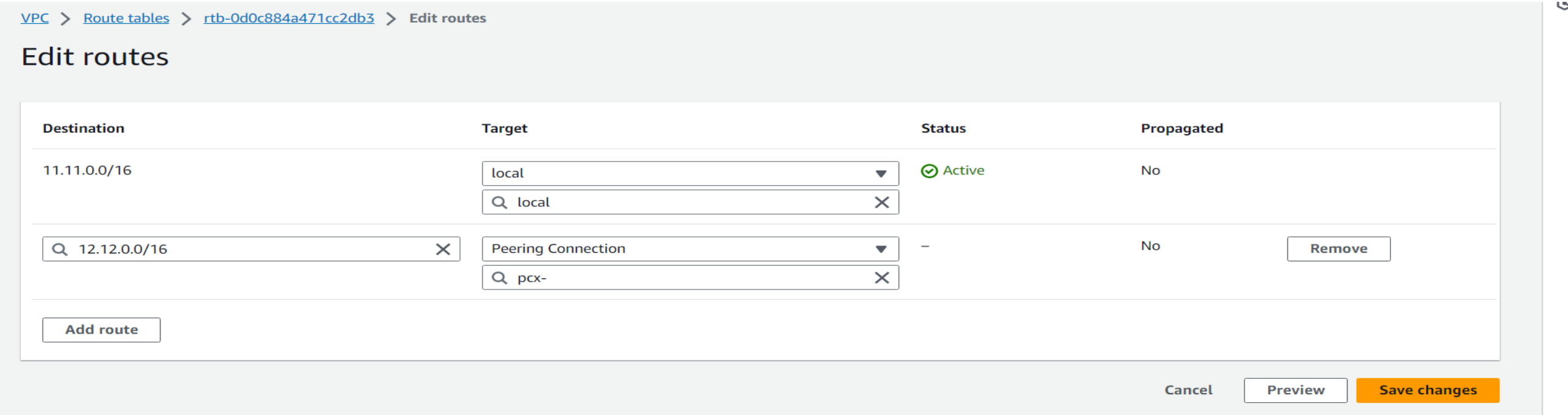
You can add 49 more tags.

Cancel | Create peering connection

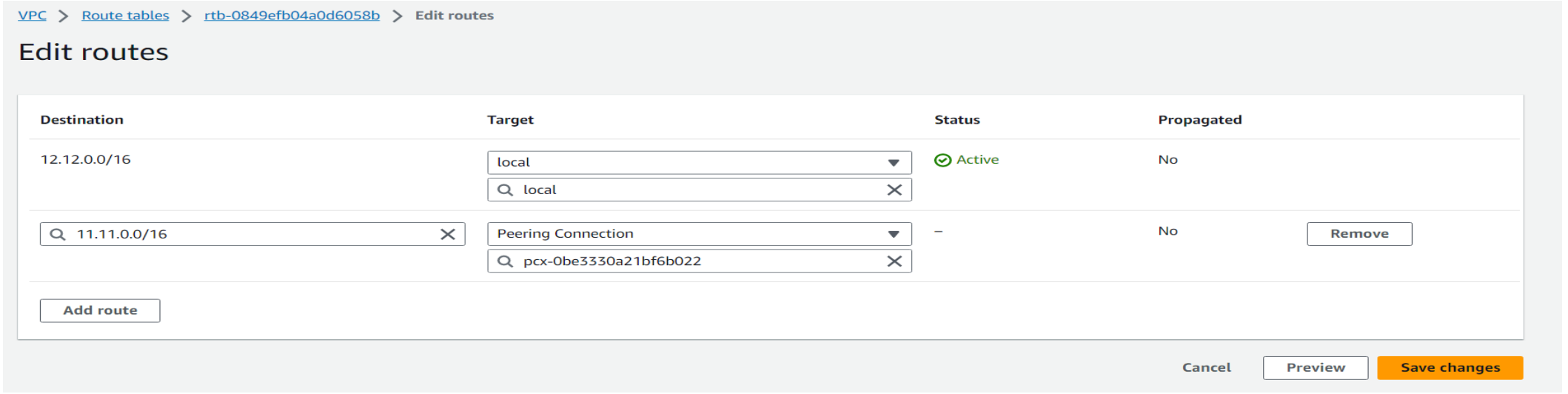
Choose the peering connection and accept the request.



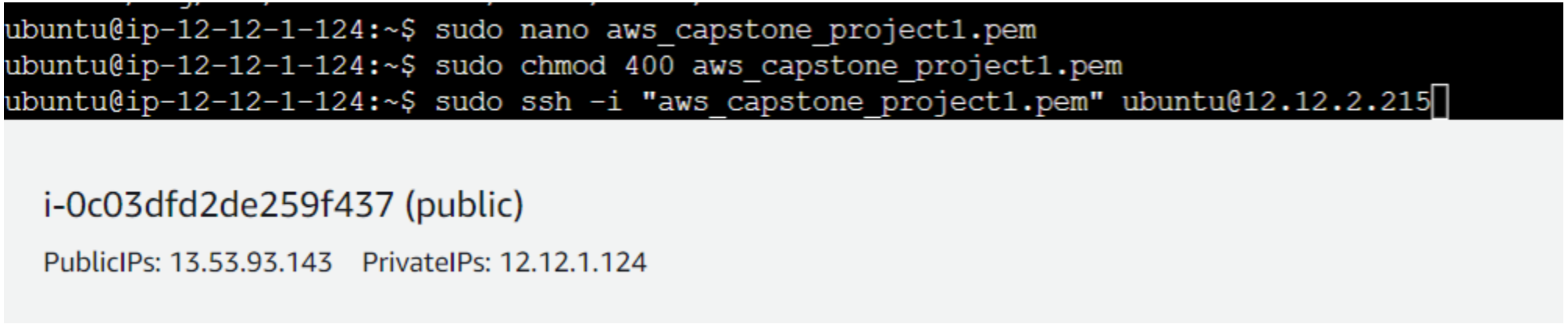
Go in vpc-1-no-int Route table – edit route –save changes.



Also do the same with vpc-2-no-int Route table.



For connecting the private subnet instance these steps need to follow .



This private subnet instance is not get updated because it doesn’t have NAT gateway. But for testing it have a peering connection we need to copy the ip of private3 instance and paste that in private instance .