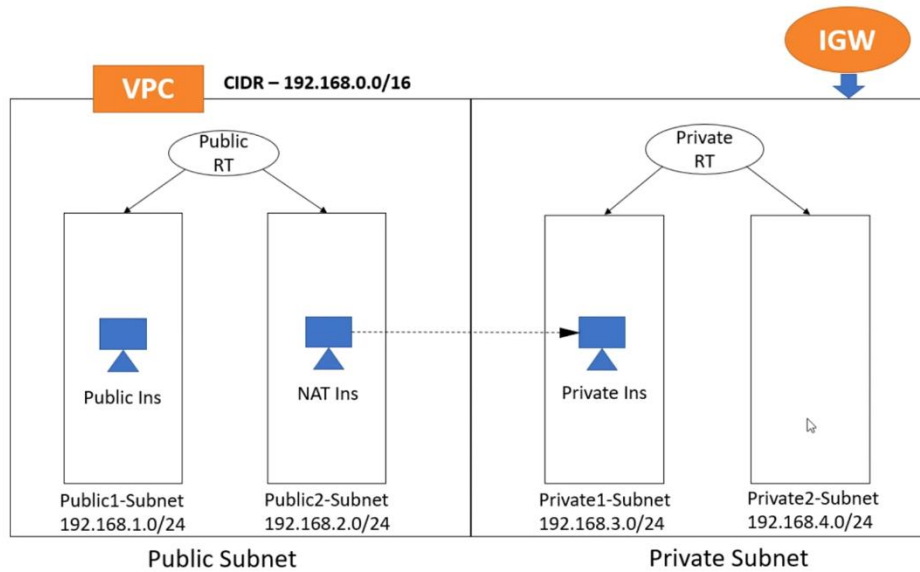


LAB 04: VPC Setup



Step 1: Create VPC: CIDR: 192.168.0.0/16

VPC dashboard ×

[EC2 Global View](#)

Filter by VPC ▾

Virtual private cloud

[VPCs](#) [NAT Gateways](#)

Create VPC [Launch EC2 Instances](#)

Note: Your instances will launch in the US West region.

Resources by Region

You are using the following Amazon VPC resources

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.

my-lab-04

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

192.168.0.0/16

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**

Q Name X Q my-lab-04 X [Remove tag](#)

[Add tag](#)

You can add 49 more tags

[Cancel](#) [Create VPC](#)

Step 2: Create Subnets:

public-subnet-1

CIDR: 192.168.1.0/24 and check the availability zone also

Subnet name

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

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.

IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block

256 IPs

public-subnet-2

CIDR: 192.168.2.0/24 and check the availability zone also

Subnet name

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

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.

IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block

256 IPs

< > ^ v

private-subnet-1

CIDR: 192.168.3.0/24 and check the availability zone also

Subnet name

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

private-subnet-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.

US West (Oregon) / us-west-2a

IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

192.168.0.0/16

IPv4 subnet CIDR block

192.168.3.0/24

256 IPs

< > ^ v

private-subnet-2

CIDR: 192.168.4.0/24 and check the availability zone also

Subnet name

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

private-subnet-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.

No preference

IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

192.168.0.0/16

IPv4 subnet CIDR block

192.168.4.0/24

256 IPs

< > ^ v

Step 3: Create Route Tables

Public-RT -select your VPC

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

VPC
The VPC to use for this route table.

vpc-028425b8e70c850e3 (my-lab-04) ▼

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	
<input type="text" value="Name"/>	<input type="text" value="Public-RT"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

Cancel

Create route table

Private-RT -select your VPC

Route table settings

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

VPC
The VPC to use for this route table.

vpc-028425b8e70c850e3 (my-lab-04) ▼

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	
<input type="text" value="Name"/>	<input type="text" value="Private-RT"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

Cancel

Create route table

Step 4: Create Internet Gateway

Internet gateway settings

Name tag

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

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

Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

Step 5: Launch an instance – Public Instance in Public Subnet - 01

Launch public EC2 instance:

Amazon Machine Image (AMI)

+

Create a new key pair

+

Edit the network setting

▼ Network settings

Info

Edit

Network | Info

vpc-09a5cf2f434230632

Subnet | Info

No preference (Default subnet in any availability zone)

Auto-assign public IP | Info

Enable

Additional charges apply when outside of free tier allowance

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

By selecting your VPC and Choose public subnet-1

Enable the Auto-assign Public IP

Create security group

Check the inbound rules

Security group name - *required*

launch-wizard-9

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-9 created 2024-09-04T17:05:32.749Z

Inbound Security Group Rules

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

Remove

Type | [Info](#)

All traffic

Protocol | [Info](#)

All

Port range | [Info](#)

All

Source type | [Info](#)

Anywhere

Source | [Info](#)

🔍 Add CIDR, prefix list or security

0.0.0.0/0 ✕

Description - *optional* | [Info](#)

e.g. SSH for admin desktop

And launch the public ec2 instance.

After launching the public EC2 instance -try to connect via EC2 instance connect...It won't work.

Step 6: To edit the routing table.

Select the Public-RT table and edit routes like 0.0.0.0/0 and select your Internet Gateway

VPC > Route tables > rtb-04823145a34895c03 > Edit routes

Edit routes

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	-	No
0.0.0.0/0	igw-051d88efb5a6f6c1a	X	No

Add route

Cancel Preview Save changes

Select the Subnet association and add both the public subnet and save the same.

Now try to connect the public EC2 instance -try to connect via EC2 instance connect...It should work.

Use ping 8.8.8.8 to test our public instance connected to the internet via IGW (created by you – user)

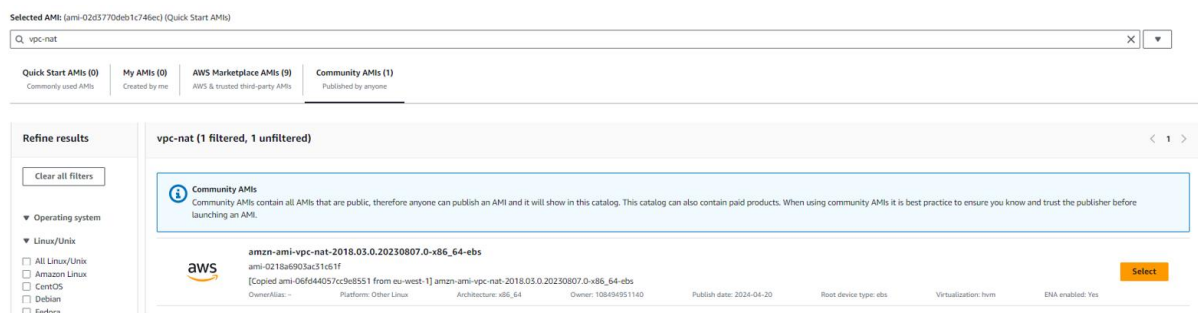
```
Amazon Linux 2023

https://aws.amazon.com/linux/amazon-linux-2023

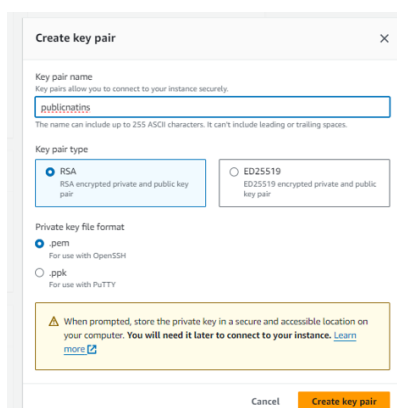
[ec2-user@ip-192-168-1-249 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=7.70 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=7.55 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=7.58 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=7.58 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=117 time=7.53 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=117 time=7.54 ms
```

Step 7: Launch an NAT instance – Public NAT Instance in Public Subnet – 02

Select the custom AMIs as mentioned below.....



Create key-pair



Choose VPC as well as subnet-2 and enable the Auto-assign public IP

Select the existing security group(You have created while creating FIRST instance) by allowing all.....

Network settings [Info](#)

VPC - required [Info](#)

vpc-028425b8e70c850e3 (my-lab-04) 192.168.0.0/16

Subnet [Info](#)

subnet-0761baf3770eb53fc public-subnet-2

VPC: vpc-028425b8e70c850e3 Owner: 339713009883 Availability Zone: us-west-2b Zone type: Availability Zone IP addresses available: 251 CIDR: 192.168.2.0/24

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of free tier allowance

Summary

Number of instances [Info](#)

1

Software Image (AMI)

amazon-ami-vpc-nat-2018.03.0.202...[read more](#)

ami-0218a6903e31e61ff

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

[Storage fundamen](#)

instance.

☐ Create security group ☒ Select existing security group

Common security groups info

Select security groups

launch-wizard-10 sg-03e93899f92c61594 X

VPC: vpc-028425b8e70c850e3

[Compare security group rules](#)

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

Public NAT Instance is ready ,will try to connect later after creating the private instance .

Step 8: Launch an ec2 instance – private Instance in Private Subnet – 01

Choose appropriate VPC , Subnet , Disable the Auto assign public IP and selecting the already created security group.

Key pair name - required

prakashpytins1

Create new key pair

▼ Network settings Info

VPC - required Info

vpc-028425b8e70c850e3 (my-lab-04)
192.168.0.0/16

Create new VPC

Subnet Info

subnet-087342183f080a227 private-subnet-1
VPC: vpc-028425b8e70c850e3 Owner: 339713009863
Availability Zone: us-west-2a Zone type: Availability Zone
IP addresses available: 251 CIDR: 192.168.3.0/24

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

launch-wizard-10 sg-03e93899f92c61594 X
VPC: vpc-028425b8e70c850e3

Compare security group rules

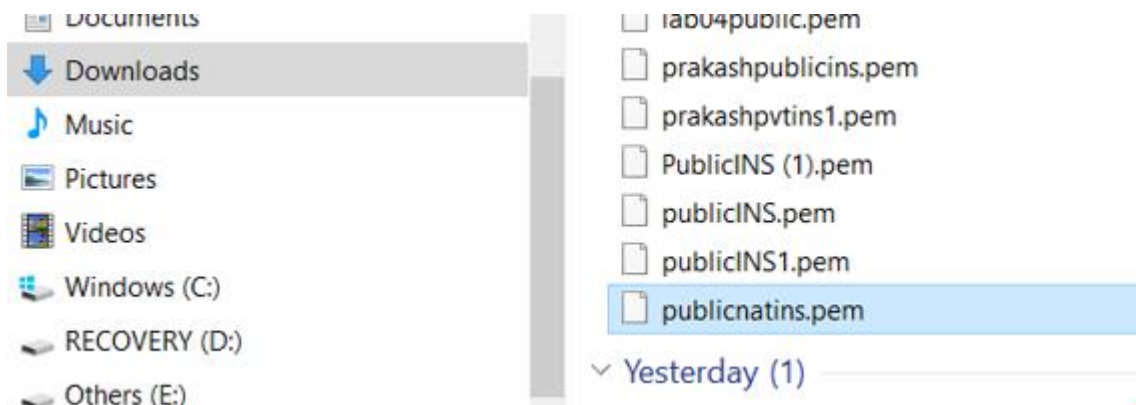
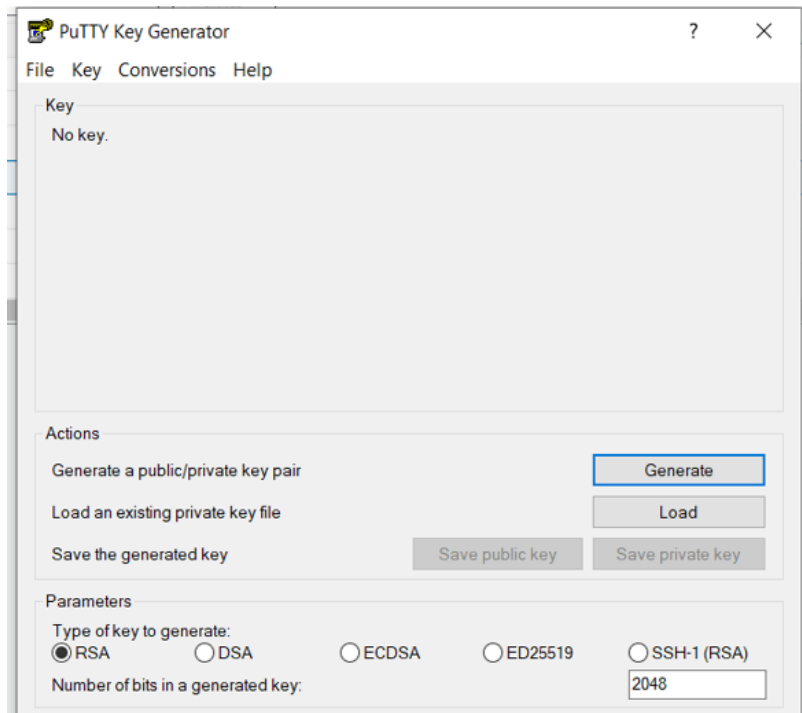
Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

Private instance is ready.

Step 09: Run a NAT instance using PUTTY Connection.

Create a KEY for NAT with the key compatibility



PutTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDchePIDR2taNyXUoZ7e/711EFYbLBQpjsCe9E9
OrciQq6eHtAKnoUm2OnJ3lqvVFKfso0KEV337ktYwlh6wJb85ccINGQmW
+v4UhVS2BkN/8YL3rkKEJ68fmGX8Bm7LrGML+WaMvHAA2b/z8zakPRITA/2VIWQdwas
+ZpT08LnQIGoTwM0mzGWwQmIfgSVGn4RSQa91f7wB9CPyJaWe
```

Key fingerprint: ssh-rsa 2048 57:24:be:b6:62:e1:3f:6d:d1:83:7f:d8:ba:a6:61:1b

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate:

☒ RSA ☐ DSA ☐ ECDSA ☐ ED25519 ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

PutTY Configuration

Category:

- Bell
- Features
- Window
- Appearance
- Behaviour
- Translation
- Selection
- Colours
- Connection
 - Data
 - Proxy
 - Telnet
 - Rlogin
 - SSH
 - Kex
 - Host keys
 - Cipher
 - Auth**
 - TTY
 - X11
 - Tunnels
 - Bugs
 - More bugs
 - Serial

Options controlling SSH authentication

☒ Display pre-authentication banner (SSH-2 only)

☐ Bypass authentication entirely (SSH-2 only)

Authentication methods

☒ Attempt authentication using Pageant

☐ Attempt TIS or CryptoCard auth (SSH-1)

☒ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding

☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

Browse...

About Help Open Cancel

ec2-user@ip-192-168-2-106:~

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

  ____|__|____)
  ____|__|____/   Amazon Linux AMI
  ____|__|____|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
16 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-2-106 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=7.32 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=7.39 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=7.43 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=7.44 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=7.36 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=58 time=7.37 ms
```

NAT instance also connected successfully.

Step 10: Connect IGW via private ec2 instance

Need to place key private pem file into NAT instance, then only NAT will help private instance to connect internet gateway.

```
C:\Users\Prakash P\Downloads>pscp -i publicnat.ppk prakashpvtins1.pem ec2-user@35.86.80.83:/home/ec2-user
```

publicnat.ppk – ppk file for nat instance

*****.pem is key for private instance

ec2-user is a default user

@followed by public IP of NAT Instance

:/home/ec2-user is the destination directory where *****.pem to be kept.

//PSCP (PuTTY Secure Copy Protocol) is a command-line tool for transferring files and folders from a Windows computer to a Linux computer

ec2-user@ip-192-168-2-106:~

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Wed Sep  4 16:08:32 2024 from 183.82.205.138

  _ |  _ |  )
  _ | (  _ /   Amazon Linux AMI
  _ |\__|__|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
16 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-2-106 ~]$ ls
prakashpvtins1.pem
```

Follow the given steps in



Connect to instance Info

Connect to your instance i-002a1eaa9576a98fc (prakashpvtINS1) using any of these options


EC2 Instance Connect Session Manager **SSH client** EC2 serial console


Instance ID

 i-002a1eaa9576a98fc (prakashpvtINS1)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is prakashpvtins1.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 `chmod 400 "prakashpvtins1.pem"`
4. Connect to your instance using its Private IP:
 192.168.3.150

Example:

 `ssh -i "prakashpvtins1.pem" ec2-user@192.168.3.150`

 **Note:** In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.


```

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
16 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-2-106 ~]$ ls
prakashpvtins1.pem
[ec2-user@ip-192-168-2-106 ~]$ chmod 400 "prakashpvtins1.pem"
[ec2-user@ip-192-168-2-106 ~]$ ssh -i "prakashpvtins1.pem" ec2-user@192.168.3.150
The authenticity of host '192.168.3.150 (192.168.3.150)' can't be established.
ECDSA key fingerprint is SHA256:tgAnNgga5PKwFIuGnVd3FW92HLwqB3dJQMvyY7sWu8A.
ECDSA key fingerprint is MD5:c0:a9:fa:ba:44:78:1c:be:53:f6:ae:fb:05:1d:36:36.
Are you sure you want to continue connecting (yes/no)? █

```

Try to ping suing ping 8.8.8.8

```

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
16 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-2-106 ~]$ ls
prakashpvtins1.pem
[ec2-user@ip-192-168-2-106 ~]$ chmod 400 "prakashpvtins1.pem"
[ec2-user@ip-192-168-2-106 ~]$ ssh -i "prakashpvtins1.pem" ec2-user@192.1
The authenticity of host '192.168.3.150 (192.168.3.150)' can't be establi
ECDSA key fingerprint is SHA256:tgAnNgga5PKwFIuGnVd3FW92HLwqB3dJQMvyY7sWu
ECDSA key fingerprint is MD5:c0:a9:fa:ba:44:78:1c:be:53:f6:ae:fb:05:1d:36
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.3.150' (ECDSA) to the list of known h

#
~\  #####_ Amazon Linux 2023
~~ \_#####\
~~  \#####|
~~   \#/
~~    V~' '-> https://aws.amazon.com/linux/amazon-linux-2023
~~
~~.
~~ \_
~~  /m/ '->
[ec2-user@ip-192-168-3-150 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
█

```

It may/may not work.

Go to Private RT table and do the route changes.

Choose 0.0.0.0/0 and select an instance as public Nat Instance and save the changes.

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
Q. 0.0.0.0/0	Q. local	X	No
	Instance	~	No
	Q. i-0523f5b2800260337	X	
	Use: i-0523f5b2800260337		
	i-0523f5b2800260337 (publicNat1)		
	i-00f0d6accfeca58c (prakashpubns1)		
	i-0b1c963bf0ad4f8aa (PBKNS-1)		

Edit the subnet associations -by adding private subnet

VPC > Route tables > [rtb-0991536204ce006bf](#) > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

Filter subnet associations

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	public-subnet-1	subnet-03342dd504c1827ec	192.168.1.0/24	-	rtb-04825145a34695c95 / Public-RT
<input type="checkbox"/>	public-subnet-2	subnet-0761ba15770eb53fc	192.168.2.0/24	-	rtb-04825145a34695c95 / Public-RT
<input checked="" type="checkbox"/>	private-subnet-1	subnet-032d55e38bca9f038	192.168.4.0/24	-	Main (rtb-06b06b24d640c761b)
<input checked="" type="checkbox"/>	private-subnet-2	subnet-087342183f080a227	192.168.3.0/24	-	Main (rtb-06b06b24d640c761b)

Selected subnets

[subnet-03342dd504c1827ec / public-subnet-1](#) [subnet-0761ba15770eb53fc / public-subnet-2](#)

Go to NAT instance change the source and destination check by enabling the STOP.

Instances (1/5) [Info](#)

Last updated less than a minute ago [Refresh](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Find Instance by attribute or tag (case-sensitive) [All states](#)

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input checked="" type="checkbox"/>	publicNATins	i-0523f5b2800260337	Running	t2.micro	2/2 checks passed	View alarms	us-west-2b	-	55.86.80.83	-
<input type="checkbox"/>	prakashpubins1	i-00f0dd6acffea68c	Running	t2.micro	2/2 checks passed	View alarms	us-west-2a	-	-	-
<input type="checkbox"/>	PBINS-1	i-0b1c963bf0ad4f8aa	Running	t2.micro	2/2 checks passed	View alarms	us-west-2a	-	-	-
<input type="checkbox"/>	lab04pubins1	i-0ec7dc0021f7ae87	Terminated	t2.micro	-	View alarms	us-west-2a	-	-	-
<input type="checkbox"/>	prakashprivtINS1	i-002a1eaa9576a98fc	Running	t2.micro	2/2 checks passed	View alarms	us-west-2a	-	-	-

Actions menu for publicNATins:

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
 - Attach network interface
 - Detach network interface
 - Connect RDS database
 - Disaster recovery for your instances
 - Change source/destination check
 - Disassociate Elastic IP address
 - Manage IP addresses
 - Manage ENA Express
- Monitor and troubleshoot

Change Source / destination check

The source / destination check ensures that the instance is the source or destination of all the traffic it sends and receives. Each EC2 instance performs source and destination checks by default. [Learn more](#)

Instance ID
[i-0523f5b2800260337](#) (publicNATins)

Network interface
[eni-0f2122094cb2aa5dc](#)

Source / destination checking
Stop to allow your instance to send and receive traffic when the source or destination is not itself.

☒ Stop

[Cancel](#) [Save](#)

Try to ping

