

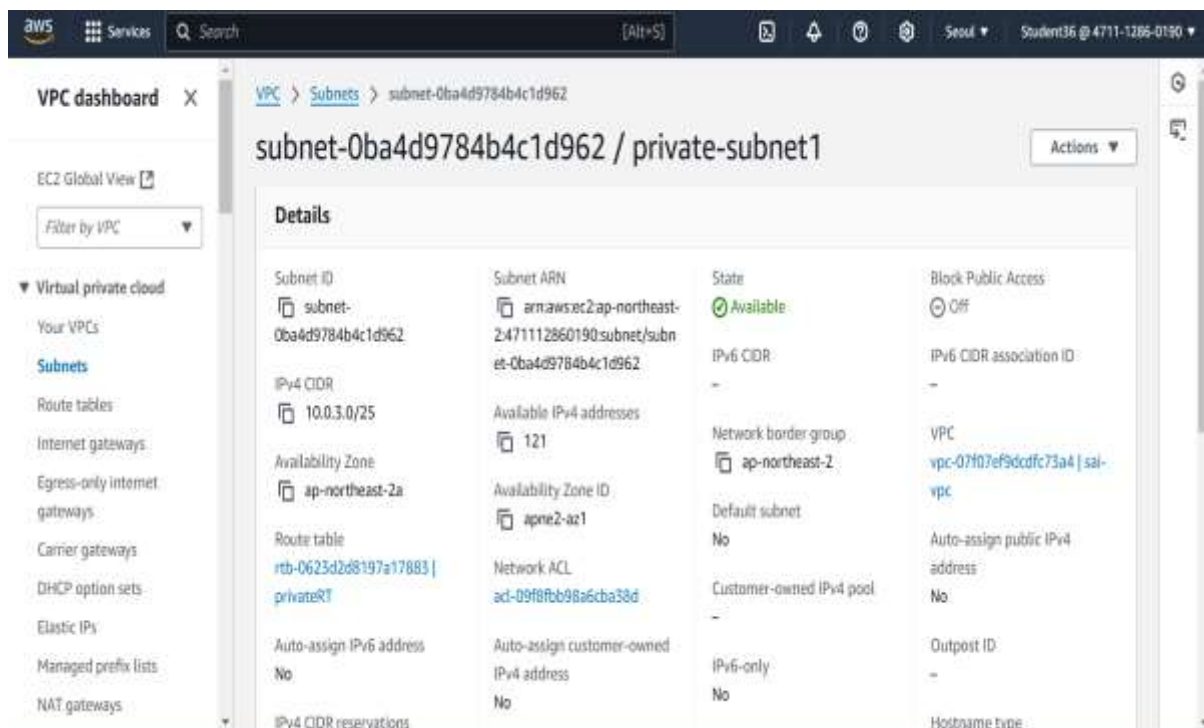
### 3.How to connect private server to internet using NAT gateway(Jump server/bastion host)

#### Create Subnets

##### Steps

1. In the VPC dashboard, select **Subnets**.
2. Click the create subnet button to create 2 public and 2 private subnets.
3. Select the VPC created.
4. Provide with the subnet name, availability zone and IPv4 subnet CIDR block for both private and public subnets.

#### Private subnet1



The screenshot shows the AWS VPC console interface. The left sidebar contains a navigation menu with options like 'Virtual private cloud', 'Your VPCs', 'Subnets', 'Route tables', 'Internet gateways', 'Egress-only internet gateways', 'Carrier gateways', 'DHCP option sets', 'Elastic IPs', 'Managed prefix lists', and 'NAT gateways'. The main content area displays the details for a specific subnet, 'subnet-0ba4d9784b4c1d962 / private-subnet1'. The details are organized into a table with four columns: Subnet ID, Subnet ARN, State, and Block Public Access. The Subnet ID is 'subnet-0ba4d9784b4c1d962', the Subnet ARN is 'arn:aws:ec2:ap-northeast-2:471112860190:subnet/subnet-0ba4d9784b4c1d962', the State is 'Available', and Block Public Access is 'Off'. Other details include IPv4 CIDR '10.0.3.0/25', Availability Zone 'ap-northeast-2a', Route table 'rtb-0623d2d8197a17883 | privateRT', Network ACL 'acl-09f8fbb98a6c38d', and Auto-assign IPv6 address 'No'.

Subnet ID	Subnet ARN	State	Block Public Access
subnet-0ba4d9784b4c1d962	arn:aws:ec2:ap-northeast-2:471112860190:subnet/subnet-0ba4d9784b4c1d962	Available	Off
IPv4 CIDR	Available IPv4 addresses	IPv6 CIDR	IPv6 CIDR association ID
10.0.3.0/25	121	-	-
Availability Zone	Availability Zone ID	Network border group	VPC
ap-northeast-2a	apne2-az1	ap-northeast-2	vpc-07f07ef9dcdcf73a4   sai-vpc
Route table	Network ACL	Default subnet	Auto-assign public IPv4 address
rtb-0623d2d8197a17883   privateRT	acl-09f8fbb98a6c38d	No	No
Auto-assign IPv6 address	Auto-assign customer-owned IPv4 address	Customer-owned IPv4 pool	Outpost ID
No	No	-	-
IPv4 CIDR reservations		IPv6-only	Hostname type
		No	

## Private subnet2

The screenshot displays the AWS Management Console interface for a VPC dashboard. The left sidebar shows the navigation menu with 'Subnets' selected. The main content area shows the details for 'subnet-0317ee604e8a105cb / private-subnet2'. The details are organized into a grid of key-value pairs.

Details			
Subnet ID	Subnet ARN	State	Block Public Access
subnet-0317ee604e8a105cb	arn:aws:ec2:ap-northeast-2:471112860190:subnet/subnet-0317ee604e8a105cb	Available	Off
IPv4 CIDR	Available IPv4 addresses	IPv6 CIDR	IPv6 CIDR association ID
10.0.4.0/25	123	-	-
Availability Zone	Availability Zone ID	Network border group	VPC
ap-northeast-2b	apne2-az2	ap-northeast-2	vpc-07f07ef9d0dfc73a4   sai-vpc
Route table	Network ACL	Default subnet	Auto-assign public IPv4 address
rtb-0625d2db197a17683   private-RT	acl-09f8fb98a6c8a38d	No	No
Auto-assign IPv6 address	Auto-assign customer-owned IPv4 address	Customer-owned IPv4 pool	Outpost ID
No	No	-	-
IPv4 CIDR reservations		IPv6-only	Hostname type
		No	-

A yellow 'Clipboard' notification is visible in the bottom right corner, stating 'Item not collected'.

## Public subnet1

The screenshot displays the AWS Management Console interface for a VPC dashboard. The left sidebar shows the navigation menu with 'Subnets' selected. The main content area shows the details for 'subnet-04448f11eb1c73935 / public-subnet1'. The details are organized into a grid of key-value pairs.

Details			
Subnet ID	Subnet ARN	State	Block Public Access
subnet-04448f11eb1c73935	arn:aws:ec2:ap-northeast-2:471112860190:subnet/subnet-04448f11eb1c73935	Available	Off
IPv4 CIDR	Available IPv4 addresses	IPv6 CIDR	IPv6 CIDR association ID
10.0.1.0/24	249	-	-
Availability Zone	Availability Zone ID	Network border group	VPC
ap-northeast-2a	apne2-az1	ap-northeast-2	vpc-07f07ef9d0dfc73a4   sai-vpc
Route table	Network ACL	Default subnet	Auto-assign public IPv4 address
rtb-0abfc9fc563362c70   public-RT	acl-09f8fb98a6c8a38d	No	No
Auto-assign IPv6 address	Auto-assign customer-owned IPv4 address	Customer-owned IPv4 pool	Outpost ID
No	No	-	-
IPv4 CIDR reservations		IPv6-only	Hostname type
		No	-

## Public subnet2

The screenshot shows the AWS VPC console interface. The left sidebar contains the 'VPC dashboard' and a list of VPC resources including 'Subnets', 'Route tables', 'Internet gateways', 'Egress-only internet gateways', 'Carrier gateways', 'DHCP option sets', 'Elastic IPs', 'Managed prefix lists', and 'NAT gateways'. The main content area displays the details for 'subnet-028aab2e0d063dfee / public-subnet2'. The details are organized into a grid:

Details	
Subnet ID subnet-028aab2e0d063dfee	Subnet ARN arn:aws:ec2:ap-northeast-2:471112860190:subnet/subnet-028aab2e0d063dfee
IPv4 CIDR 10.0.2.0/24	Available IPv4 addresses 251
Availability Zone ap-northeast-2b	Availability Zone ID apne2-az2
Route table rtb-0abfc9fc563362c70   public-RT	Network ACL acl-098bfbh9fa6cha38d
Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No
IPv6 CIDR reservations	
State Available	Block Public Access Off
IPv6 CIDR	IPv6 CIDR association ID
Network border group ap-northeast-2	VPC vpc-07f07ef9d0dc71a4   sai-vpc
Default subnet No	Auto-assign public IPv4 address No
Customer-owned IPv4 pool	Outpost ID
IPv6-only No	Hostname type

## Create Route Table

### Steps

1. In the VPC dashboard, select **Route Table**.
2. Click the create route table button.
3. Provide the name as neha-private-RT and the created VPC.
4. Under the Subnet Association, click Edit subnet association.
5. Check the private subnets and save association.

The screenshot shows the AWS VPC console interface. The left sidebar contains the 'VPC dashboard' and a list of VPC resources including 'Subnets', 'Route tables', 'Internet gateways', 'Egress-only internet gateways', 'Carrier gateways', 'DHCP option sets', 'Elastic IPs', 'Managed prefix lists', and 'NAT gateways'. The main content area displays the details for 'rtb-09e5a7edf84825b9e / sai-private-RT'. The details are organized into a grid:

Details	
Route table ID rtb-09e5a7edf84825b9e	Main No
VPC vpc-06afa614053262a9b   sai-vpc	Explicit subnet associations 2 subnets
Owner ID 471112860190	Edge associations

Below the details, there are tabs for 'Routes', 'Subnet associations', 'Edge associations', 'Route propagation', and 'Tags'. The 'Routes' tab is selected, showing a list of routes:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

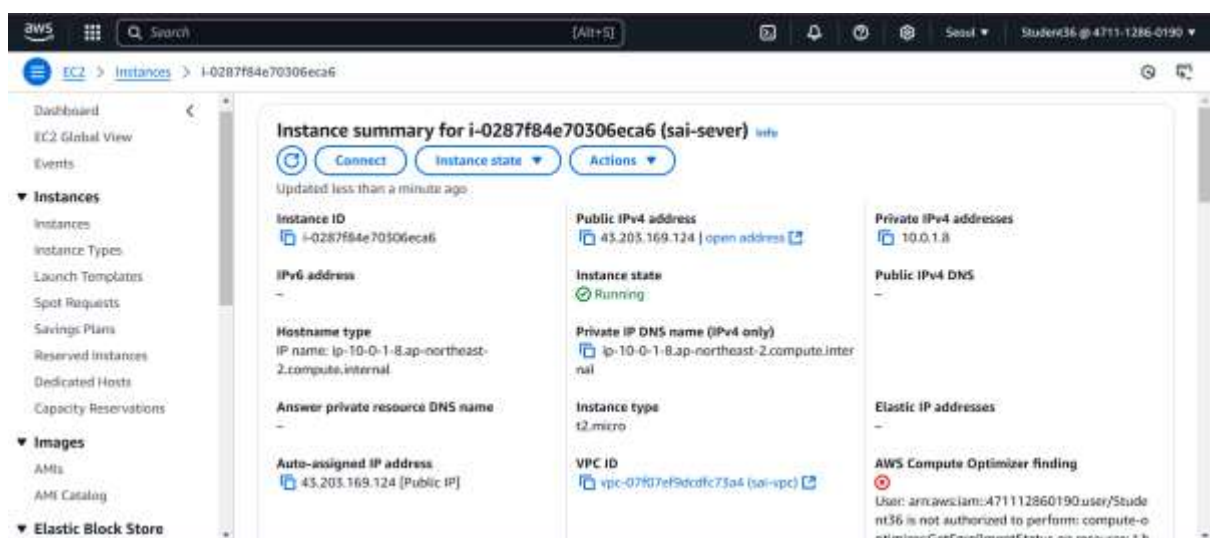
## Create NAT gateway

### Steps

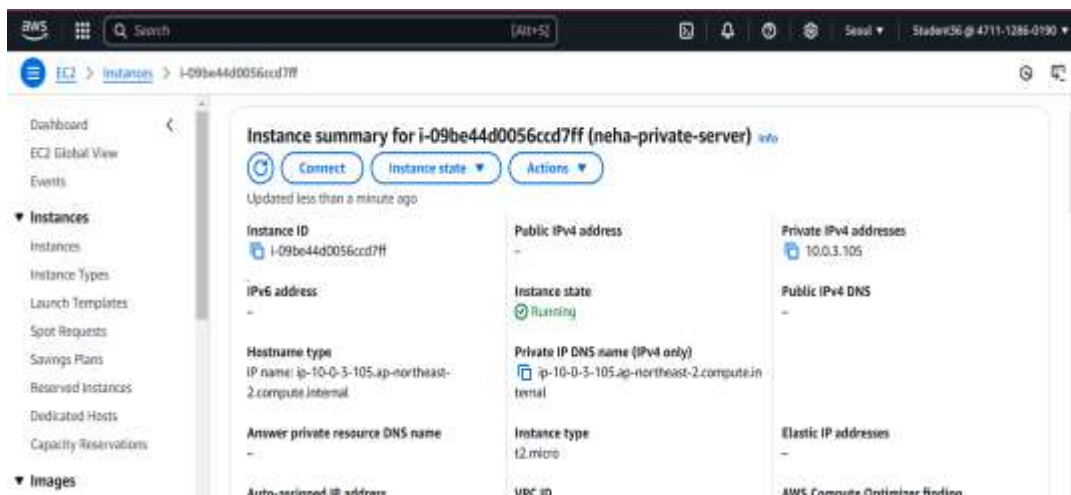
1. In the VPC dashboard, select **NAT Gateways**.
2. Click the create NAT Gateway.
3. Provide the name as sai-natgateway and select the created public subnet and the allocate Elastic IP allocation ID.
4. In the route table check the private-RT and provide the target as NAT gateway.



## Create public server



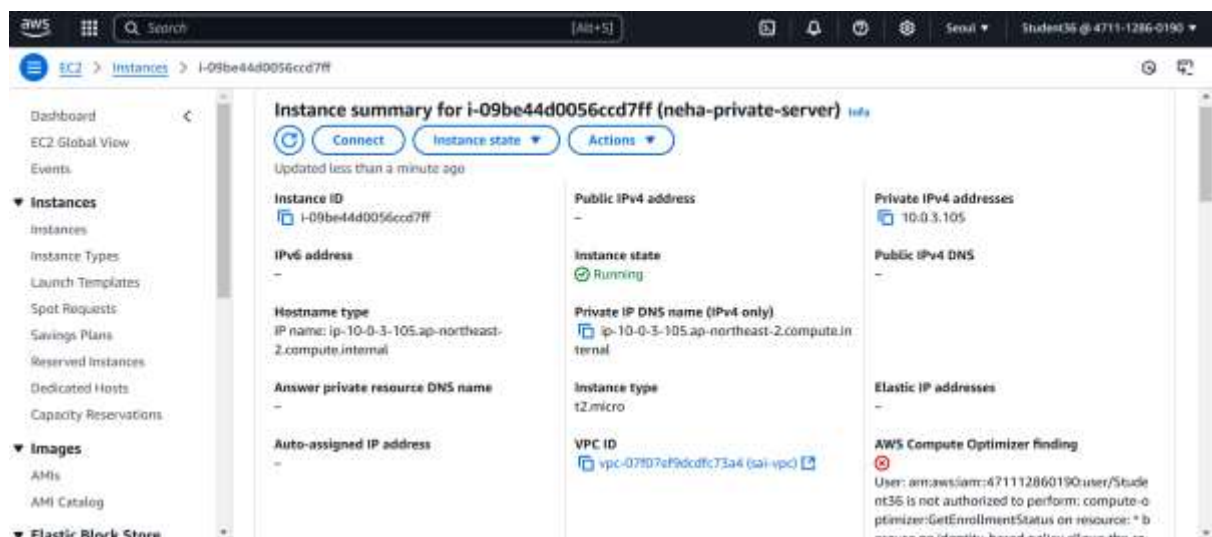
## Create Public server



## Create Private server

### Steps

1. In EC2 dashboard, select instance and click Launch instances.
2. Provide the name as sai-private-server and create a private keypair.
3. Select the appropriate VPC and provide the security group as sai-private-server-SG.
4. Launch the instance.





## Final result

Open the command prompt and provide the following commands

### 1. cd downloads

```
Microsoft Windows [version 10.0.19045.4651]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nhaa.DESKTOP-HP73721>cd Downloads

C:\Users\nhaa.DESKTOP-HP73721\Downloads>ssh -i "nha-private-keypair.pem" ec2-user@10.0.3.105
ssh: connect to host 10.0.3.105 port 22: Connection timed out

C:\Users\nhaa.DESKTOP-HP73721\Downloads>ssh -i "nha-private-keypair.pem" ec2-user@10.0.3.105
ssh: connect to host 10.0.3.105 port 22: Connection timed out

C:\Users\nhaa.DESKTOP-HP73721\Downloads>ssh -i "sai-keypair.pem" ec2-user@43.203.169.124
ssh: connect to host 43.203.169.124 port 22: Connection timed out

C:\Users\nhaa.DESKTOP-HP73721\Downloads>ssh -i "sai-keypair.pem" ec2-user@43.203.169.124

Amazon Linux 2023

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

Last login: Tue Dec 10 04:41:59 2024 from 223.186.226.153
[ec2-user@ip-10-0-1-36 ~]$ sudo su
[root@ip-10-0-1-36 ec2-user]# cd
[root@ip-10-0-1-36 ~]# ssh -i "nha-private-keypair.pem" ec2-user@10.0.3.105
Warning: Identity file nha-private-keypair.pem not accessible: No such file or directory.
The authenticity of host "10.0.3.105 (10.0.3.105)" can't be established.
ED25519 key fingerprint is SHA256:WQcTichmXtopyWwDIDAP1rPp2Yud5ilct9Msc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added "10.0.3.105" (ED25519) to the list of known hosts.
ec2-user@10.0.3.105: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[root@ip-10-0-1-36 ~]# vi nha-private-keypair.pem
[root@ip-10-0-1-36 ~]# ssh -i "nha-private-keypair.pem" ec2-user@10.0.3.105
Warning: UNPROTECTED PRIVATE KEY FILE!

ec2-user@ip-10-0-1-36~$
[ec2-user@ip-10-0-1-36 ~]$ ping www.google.com
PING www.google.com (142.250.191.196) 56(84) bytes of data:
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=1 ttl=117 time=8.41 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=2 ttl=117 time=8.64 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=3 ttl=117 time=8.75 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=4 ttl=117 time=8.39 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=5 ttl=117 time=8.56 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=6 ttl=117 time=8.48 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=7 ttl=117 time=8.67 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=8 ttl=117 time=8.42 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=9 ttl=117 time=9.11 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=10 ttl=117 time=8.84 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=11 ttl=117 time=8.75 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=12 ttl=117 time=8.57 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=13 ttl=117 time=8.71 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=14 ttl=117 time=8.68 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=15 ttl=117 time=8.47 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=16 ttl=117 time=8.69 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=17 ttl=117 time=8.43 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=18 ttl=117 time=9.18 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=19 ttl=117 time=8.50 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=20 ttl=117 time=9.00 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=21 ttl=117 time=8.46 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=22 ttl=117 time=8.64 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=23 ttl=117 time=8.45 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=24 ttl=117 time=8.91 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=25 ttl=117 time=8.87 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=26 ttl=117 time=8.42 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=27 ttl=117 time=8.68 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=28 ttl=117 time=8.58 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=29 ttl=117 time=8.62 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=30 ttl=117 time=8.96 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=31 ttl=117 time=8.76 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=32 ttl=117 time=8.76 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=33 ttl=117 time=8.92 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=34 ttl=117 time=8.98 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=35 ttl=117 time=8.66 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=36 ttl=117 time=8.46 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=37 ttl=117 time=8.64 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=38 ttl=117 time=8.68 ms
64 bytes from ord38a31-in-f4.1e100.net (142.250.191.196): icmp_seq=39 ttl=117 time=8.45 ms
```