

NETWORK ADDRESS TRANSLATION (NAT) GATEWAY

An **AWS NAT Gateway** is a managed Network Address Translation (NAT) service that enables instances in a private subnet to connect to the internet or other AWS services, while preventing external systems from initiating connections to those instances. This setup is essential for scenarios where resources require outbound access without exposing them to unsolicited inbound traffic.

Types of NAT Gateways:

1. Public NAT Gateway:

- **Purpose:** Allows instances in private subnets to access the internet.
- **Configuration:** Deployed in a public subnet with an associated Elastic IP address.
- **Routing:** Traffic from private subnets is routed to the NAT Gateway, which then communicates with the internet via an Internet Gateway.

2. Private NAT Gateway:

- **Purpose:** Enables instances in private subnets to connect to other VPCs or on-premises networks without using the internet.
- **Configuration:** Deployed in a private subnet without an Elastic IP address.
- **Routing:** Traffic is routed through a Transit Gateway or Virtual Private Gateway to reach desired networks.

In AWS, both **NAT Gateways** and **NAT Instances** serve the purpose of enabling instances in private subnets to initiate outbound IPv4 traffic to the internet or other AWS services, while preventing unsolicited inbound traffic from external sources. Here's a comparison of the two:

NAT Gateway:

- **Managed Service:** AWS manages the deployment, maintenance, and scaling, reducing administrative overhead.
- **High Availability:** Designed with redundancy within each Availability Zone (AZ). For zone-independent architecture, deploy a NAT Gateway in each AZ.
- **Scalability:** Automatically scales up to 100 Gbps to accommodate varying traffic levels.
- **Cost:** Involves charges based on usage duration and data processed.
- **Security:** Cannot be associated with security groups; control traffic using Network ACLs.

NAT Instance:

- **Self-Managed:** Requires manual setup, configuration, and maintenance, including software updates and patches.
- **Availability:** Achieving high availability necessitates configuring failover between instances, often using scripts.
- **Scalability:** Limited by the instance type's bandwidth; scaling may require resizing or adding instances.
- **Cost:** Costs are based on the instance type, size, and duration of operation.
- **Security:** Can be associated with security groups to control inbound and outbound traffic.

Key Differences:

- **Management:** NAT Gateways are fully managed by AWS, whereas NAT Instances require user management.
- **Performance:** NAT Gateways offer higher bandwidth and automatic scaling; NAT Instances are constrained by the chosen instance's capacity.
- **Maintenance:** NAT Gateways require minimal maintenance; NAT Instances necessitate regular administrative tasks.
- **Security Configuration:** NAT Instances allow for security group associations; NAT Gateways do not.

Creating a **Virtual Private Cloud (VPC)** with a **Network Address Translation (NAT)** Gateway in AWS allows instances in private subnets to access the internet securely.

Go to **AWS** console Management:

1. Create a VPC:

- Navigate to the **VPC Dashboard** in the AWS Management Console.
- Click on **"Create VPC"**.
- Provide a **Name** and specify an **IPv4 CIDR block** (e.g., **10.200.0.0/16**).
- Choose **"Create"** to establish the 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.

NAT

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

IPv4 CIDR
10.200.0.0/16
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
☒ No IPv6 CIDR block

VPC created successfully

Your VPCs (1/2) Info

Last updated less than a minute ago

Name	VPC ID	State	Block Public...	IPv4 CIDR
-	vpc-03c4ef00c4d76e0aa	Available	Off	172.31.0.0/16
NAT-VPC	vpc-038878515544c4b6a	Available	Off	10.200.0.0/16

vpc-038878515544c4b6a / NAT-VPC

Details Resource map CIDRs Flow logs Tags Integrations

Details

VPC ID vpc-038878515544c4b6a State Available

Block Public Access Off

DNS hostnames Disabled

2. Create and Attach an Internet Gateway:

- In the VPC Dashboard, select **"Internet Gateways"** and click **"Create Internet Gateway"**.
- Provide a **Name** and choose **"Create"**.
- Select the newly created Internet Gateway, click **"Actions"**, and choose **"Attach to VPC"**
- Select your VPC and confirm the attachment.

The screenshot shows the AWS Management Console interface for creating a new internet gateway. The breadcrumb navigation at the top reads 'VPC > Internet gateways > Create internet gateway'. The main heading is 'Create internet gateway' with an 'Info' link. Below this is a descriptive sentence: '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.' The 'Internet gateway settings' section contains a 'Name tag' field with the value 'NAT-IGW'. The 'Tags - optional' section shows a table with one tag: 'Name' as the key and 'NAT-IGW' as the value. At the bottom right, there are 'Cancel' and 'Create internet gateway' buttons. A Windows watermark is visible in the bottom right corner.

aws [Search] [Alt+S] Asia Pacific (Mumbai) Kavitha

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.

NAT-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	NAT-IGW	Remove

[Add new tag](#)
You can add 49 more tags.

[Cancel](#) [Create internet gateway](#)

Activate Windows
Go to Settings to activate Windows.

Attach the Internet gateway to VPC

The screenshot shows the AWS Management Console interface for attaching an existing internet gateway to a VPC. The breadcrumb navigation at the top reads 'VPC > Internet gateways > Attach to VPC (igw-00b21c40117b0179c)'. A green notification banner at the top states: 'The following internet gateway was created: igw-00b21c40117b0179c - NAT-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.' The main heading is 'Attach to VPC (igw-00b21c40117b0179c)' with an 'Info' link. The 'VPC' section contains a description: 'Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.' The 'Available VPCs' section shows a search bar with the value 'vpc-038878515544c4b6a'. At the bottom right, there are 'Cancel' and 'Attach internet gateway' buttons.

aws [Search] [Alt+S] Asia Pacific (Mumbai) Kavitha

VPC > Internet gateways > Attach to VPC (igw-00b21c40117b0179c)

✓ The following internet gateway was created: igw-00b21c40117b0179c - NAT-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet. [Attach to a VPC](#)

Attach to VPC (igw-00b21c40117b0179c) [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-038878515544c4b6a

AWS Command Line Interface command

[Cancel](#) [Attach internet gateway](#)

3. Create Subnets:

- **Public Subnet:**

- In the VPC Dashboard, select "**Subnets**" and click "**Create Subnet**".
- Assign a **Name**, select the **VPC** created earlier, and specify an **IPv4 CIDR block** (e.g., **10.200.0.0/24**).
- Designate an **Availability Zone** as needed.
- Ensure **Auto-assign public IPv4 address** is **enabled**.

- **Private Subnet:**

- Repeat the steps above to create another subnet.
- Assign a **Name**, select the **same VPC**, and specify a different **IPv4 CIDR block** (e.g., **10.200.1.0/24**).
- Ensure **Auto-assign public IPv4 address** is **disabled**.

The screenshot shows the 'Create subnet' page in the AWS Management Console for 'Subnet 1 of 1'. The page title is 'Subnet settings' with a subtitle 'Specify the CIDR blocks and Availability Zone for the subnet.' The form includes the following fields:

- Subnet name:** A text input field containing 'NAT-PUB-SN'. Below it, a note states 'The name can be up to 256 characters long.'
- Availability Zone:** A dropdown menu showing 'Asia Pacific (Mumbai) / ap-south-1a'.
- IPv4 VPC CIDR block:** A dropdown menu showing '10.200.0.0/16'.
- IPv4 subnet CIDR block:** A text input field containing '10.200.0.0/24'. To the right of the field, it says '256 IPs'.

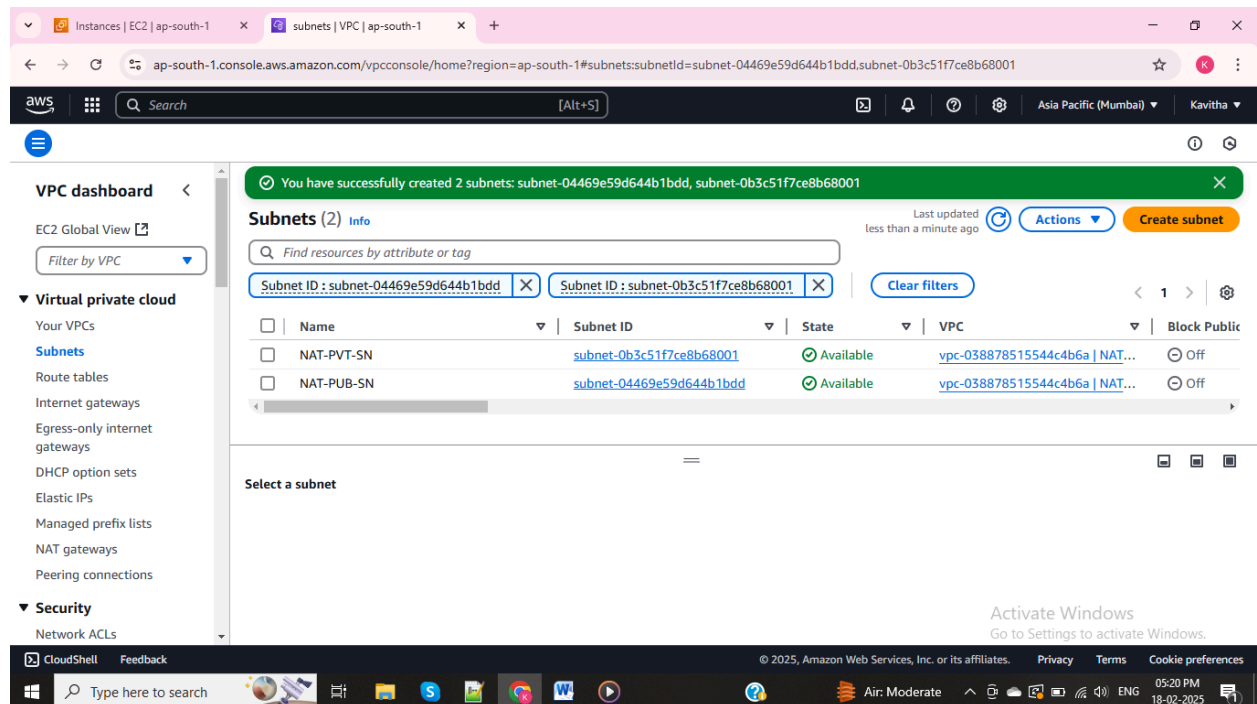
At the bottom, there is a section for 'Tags - optional' which is currently collapsed. An 'Activate Windows' watermark is visible in the bottom right corner.

The screenshot shows the 'Create subnet' page in the AWS Management Console for 'Subnet 2 of 2'. The page title is 'Subnet settings' with a subtitle 'Specify the CIDR blocks and Availability Zone for the subnet.' The form includes the following fields:

- Subnet name:** A text input field containing 'NAT-PVT-SN'. Below it, a note states 'The name can be up to 256 characters long.'
- Availability Zone:** A dropdown menu showing 'Asia Pacific (Mumbai) / ap-south-1b'.
- IPv4 VPC CIDR block:** A dropdown menu showing '10.200.0.0/16'.
- IPv4 subnet CIDR block:** A text input field containing '10.200.1.0/24'. To the right of the field, it says '256 IPs'.

At the bottom, there is a section for 'Tags - optional' which is expanded. It shows a table with two columns: 'Key' and 'Value - optional'. The first row has the key 'Name' and the value 'NAT-PVT-SN'. There is a 'Remove' button next to the value. An 'Activate Windows' watermark is visible in the bottom right corner.

Public and private subnets created successfully



4. Configure Route Tables:

● Public Route Table:

- In the VPC Dashboard, select "**Route Tables**" and click "**Create Route Table**".
- Assign a **Name**, select your **VPC**, and choose "**Create**".
- With the new route table selected, navigate to the "**Routes**" tab and click "**Edit routes**".
- Add a route with **Destination** **0.0.0.0/0** and **Target** as the Internet Gateway.
- Save the changes.
- Navigate to the "**Subnet Associations**" tab, click "**Edit subnet associations**", and associate the **public subnet**.

● Private Route Table:

- Repeat the steps to create another route table for the private subnet.
- No routes need to be added at this stage.
- Associate this route table with the **private subnet**.

Public Route Table

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

Kavitha

VPC > Route tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

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

NAT-PUB-RT

VPC
The VPC to use for this route table.

vpc-038878515544c4b6a (NAT-VPC)

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

Q Name X

Value - optional

Q NAT-PUB-RT X Remove

Add new tag

You can add 49 more tags.

Activate Windows
Go to Settings to activate Windows.

Private Route Table

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

Kavitha

VPC > Route tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

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

NAT-PVT-RT

VPC
The VPC to use for this route table.

vpc-038878515544c4b6a (NAT-VPC)

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

Q Name X

Value - optional

Q NAT-PVT-RT X Remove

Add new tag

You can add 49 more tags.

Activate Windows
Go to Settings to activate Windows.

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

Kavitha

VPC > Route tables > rtb-0d1517113d3f48f44 > 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
<input type="checkbox"/>	NAT-PVT-SN	subnet-0b3c51f7ce8b68001	10.200.1.0/24	-	Main (rtb-0931db636ccd9d5ef)
<input checked="" type="checkbox"/>	NAT-PUB-SN	subnet-04469e59d644b1bdd	10.200.0.0/24	-	Main (rtb-0931db636ccd9d5ef)

Selected subnets

subnet-04469e59d644b1bdd / NAT-PUB-SN X

Cancel Save associations

5. Create a NAT Gateway:

- In the VPC Dashboard, select **"NAT Gateways"** and click **"Create NAT Gateway"**.
- Assign a **Name**, select the **public subnet**, and allocate a new **Elastic IP**.
- Choose **"Create NAT Gateway"**.

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateNatGateway:

VPC > NAT gateways > Create NAT gateway

✓ Elastic IP address 3.111.84.194 (eipalloc-04bd7a3e1fa82a492) allocated.

Create NAT gateway [Info](#)

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

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

NAT-GW

The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.

subnet-04469e59d644b1bdd (NAT-PUB-SN)

Connectivity type
Select a connectivity type for the NAT gateway.

☒ Public
☐ Private

Elastic IP allocation ID [Info](#)
Assign an Elastic IP address to the NAT gateway.

eipalloc-04bd7a3e1fa82a492

[Allocate Elastic IP](#)

Activate Windows
Go to Settings to activate Windows.

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

05:24 PM
18-02-2025

NAT GATEWAY created successfully

aws

Search [Alt+S]

Asia Pacific (Mumbai) Kavitha

VPC dashboard <

EC2 Global View

Filter by VPC

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

▼ Security

Network ACLs

✓ NAT gateway nat-08a25b0d637233c29 | NAT-GW was created successfully.

NAT gateways (1) [Info](#)

[Find resources by attribute or tag](#)

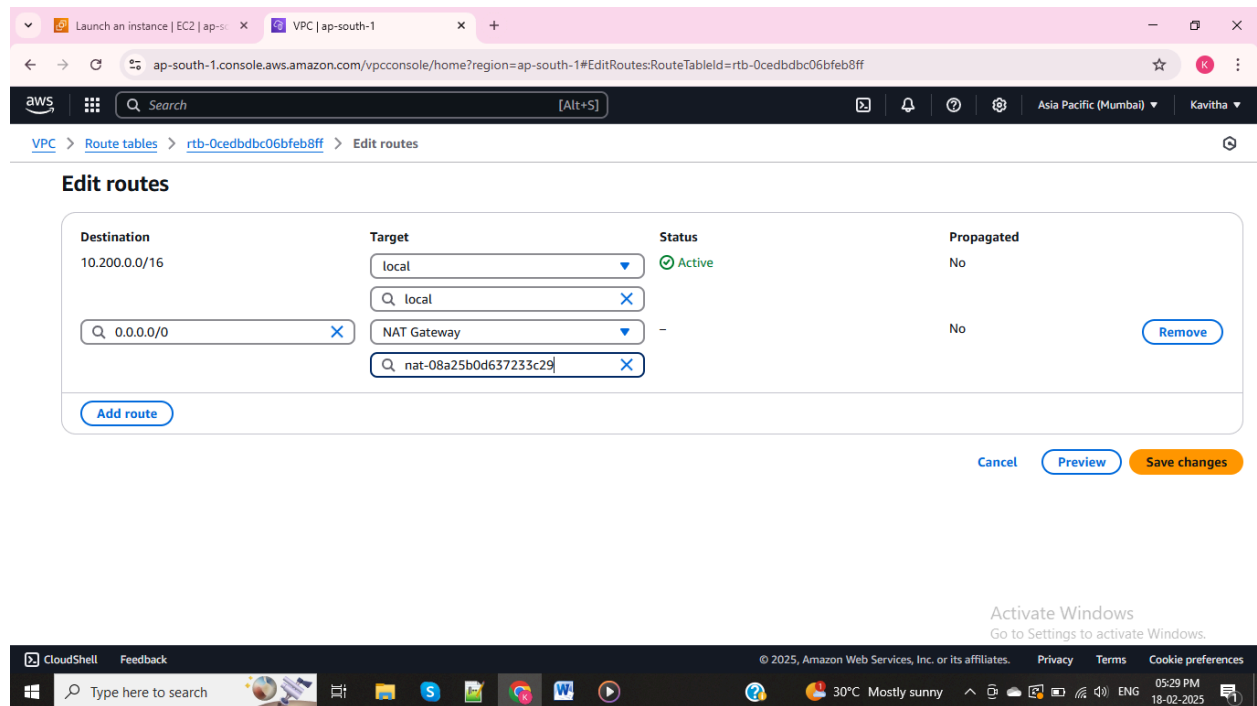
Name	NAT gateway ID	Connectivity...	State	State message	Primary public I...
NAT-GW	nat-08a25b0d637233c29	Public	✓ Available	-	3.111.84.194

Select a NAT gateway

Activate Windows
Go to Settings to activate Windows.

6. Update Private Route Table:

- Select the **private route table** created earlier.
- Navigate to the **"Routes"** tab and click **"Edit routes"**.
- Add a route with **Destination** **0.0.0.0/0** and **Target** as the NAT Gateway.
- Save the changes.



To enable secure communication between instances in a private subnet and those in a public subnet within your Virtual Private Cloud (VPC).

1. Launch a Public Instance

Purpose: Serves as an intermediary, allowing secure SSH access to instances in the private subnet.

Steps:

- Launch an EC2 instance in the **public subnet** of created VPC.
- Assign it a **public IP address**
- Attach a **security group** that permits inbound SSH (port 22) access.

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name
NAT-PUB [Add additional tags](#)

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents **Quick Start**

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux De [Browse more AMIs](#)

Summary

Number of instances [Info](#)
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-0ddfb243cbee3768

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

[Cancel](#) [Launch instance](#)

Activate Windows [Go to Settings to activate Windows.](#)

Network settings [Info](#)

VPC - required [Info](#)
vpc-038878515544c4b6a (NAT-VPC)
10.200.0.0/16

Subnet [Info](#)
subnet-04469e59d644b1bdd NAT-PUB-SN
VPC: vpc-038878515544c4b6a Owner: 476114123923
Availability Zone: ap-south-1a Zone type: Availability Zone
IP addresses available: 250 CIDR: 10.200.0.0/24 [Create new subnet](#)

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

Security group name - required
launch-wizard-1
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 _-./!@#%&*~

Summary

Number of instances [Info](#)
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-0ddfb243cbee3768

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

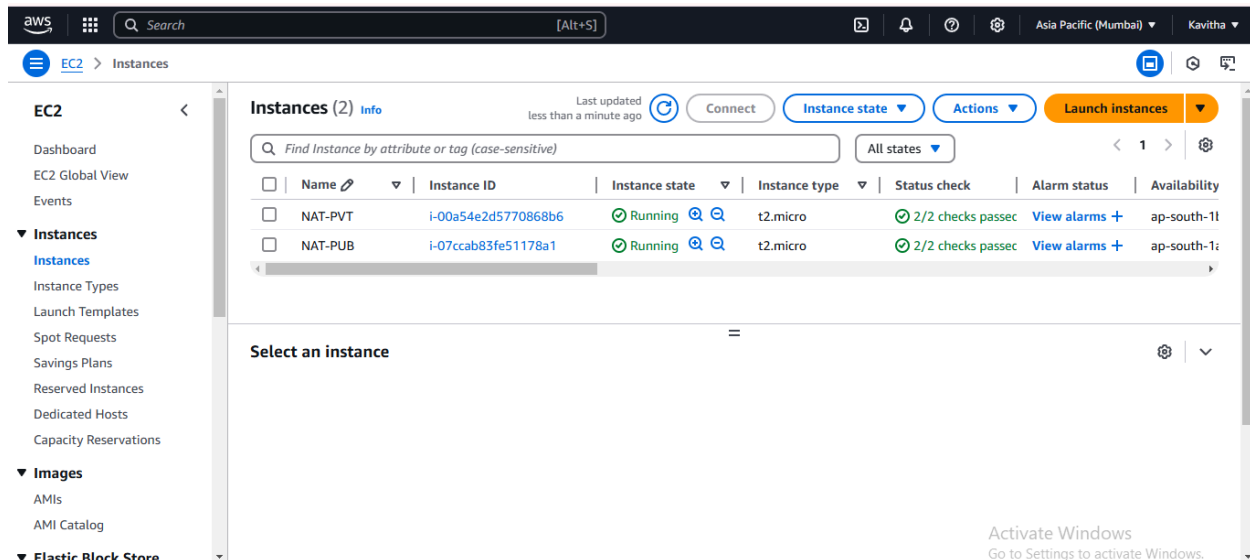
[Cancel](#) [Launch instance](#)

Activate Windows [Go to Settings to activate Windows.](#)

2. Launch a Private Instance:

- **Purpose:** The target instance residing in the private subnet without direct internet exposure.
- **Steps:**
 - Launch an EC2 instance in the **private subnet** of created VPC.
 - Ensure it does **not** have a public IP address.
 - Attach a **security group** that allows inbound SSH (port 22) traffic from the **public instance's security group**.

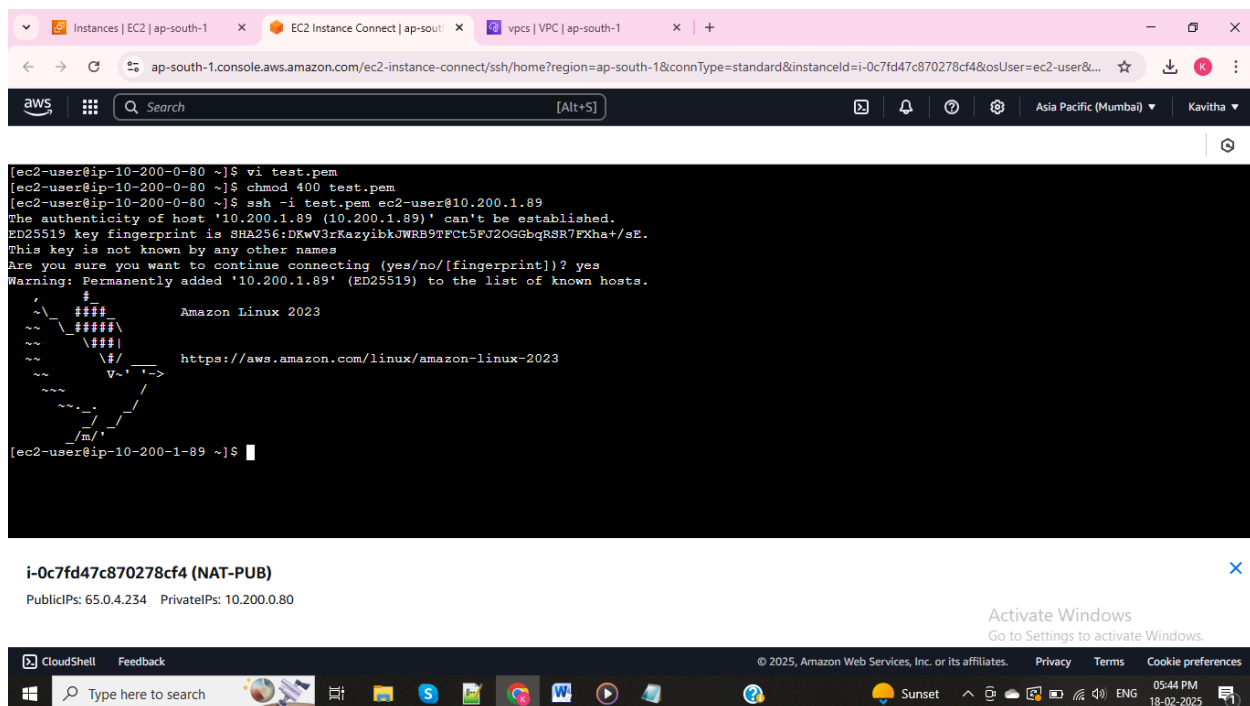
Public and Private Instance created



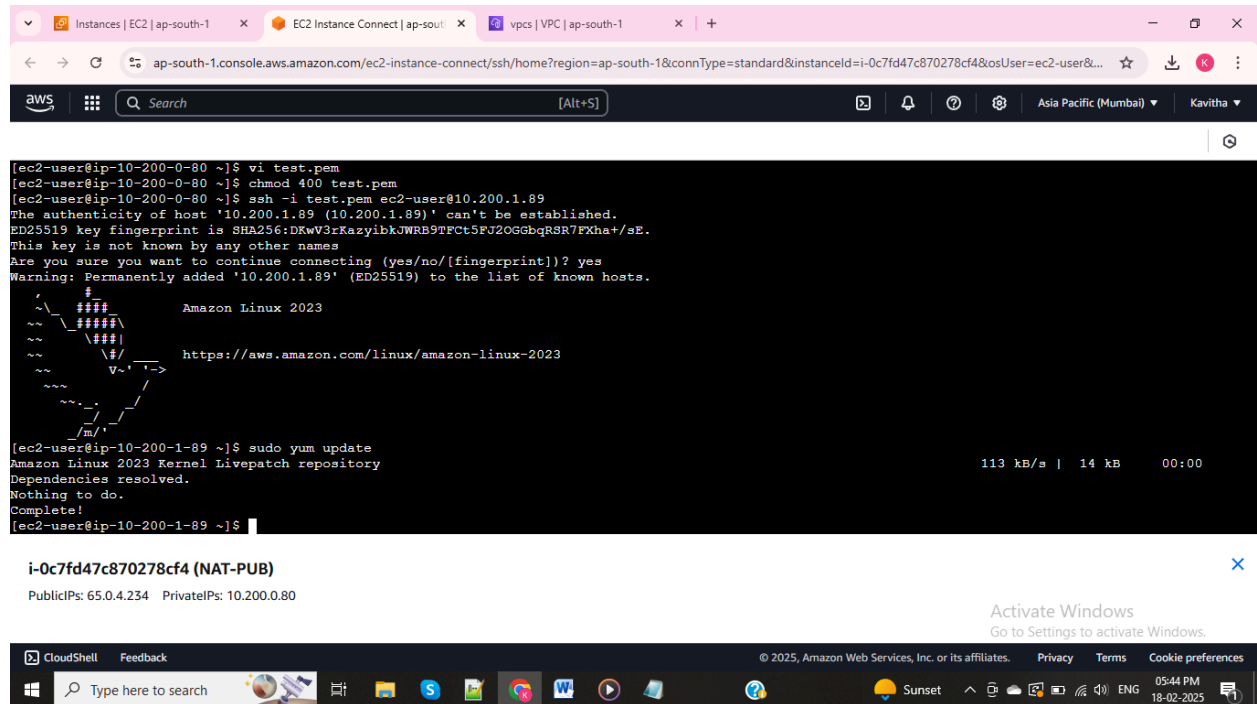
Connect the **Public Instance** --> Update the server --> Create a **.pem** file and Key was pasted in that file and save.

Change permission for the key --> **chmod 400 test.pem**

To connect private Instance give --> **ssh -i test.pem ec2-user@(private Ip of private Instance)**



Inside private Instance, server was updated by **sudo yum update**



Checking the Internet by ping google.com

