**AWS VPC Setup: Bastion Host, NAT Gateway, and Private EC2**

**Author**: DEVANSH SHARMA (11721210014)

**Submitted To**: HIMANSU SIR

**Date**: May 18, 2025

**Introduction**

This document describes the step-by-step creation of an AWS infrastructure consisting of a public and private subnet, a bastion host, a NAT Gateway, and a backend EC2 instance, within a custom VPC.

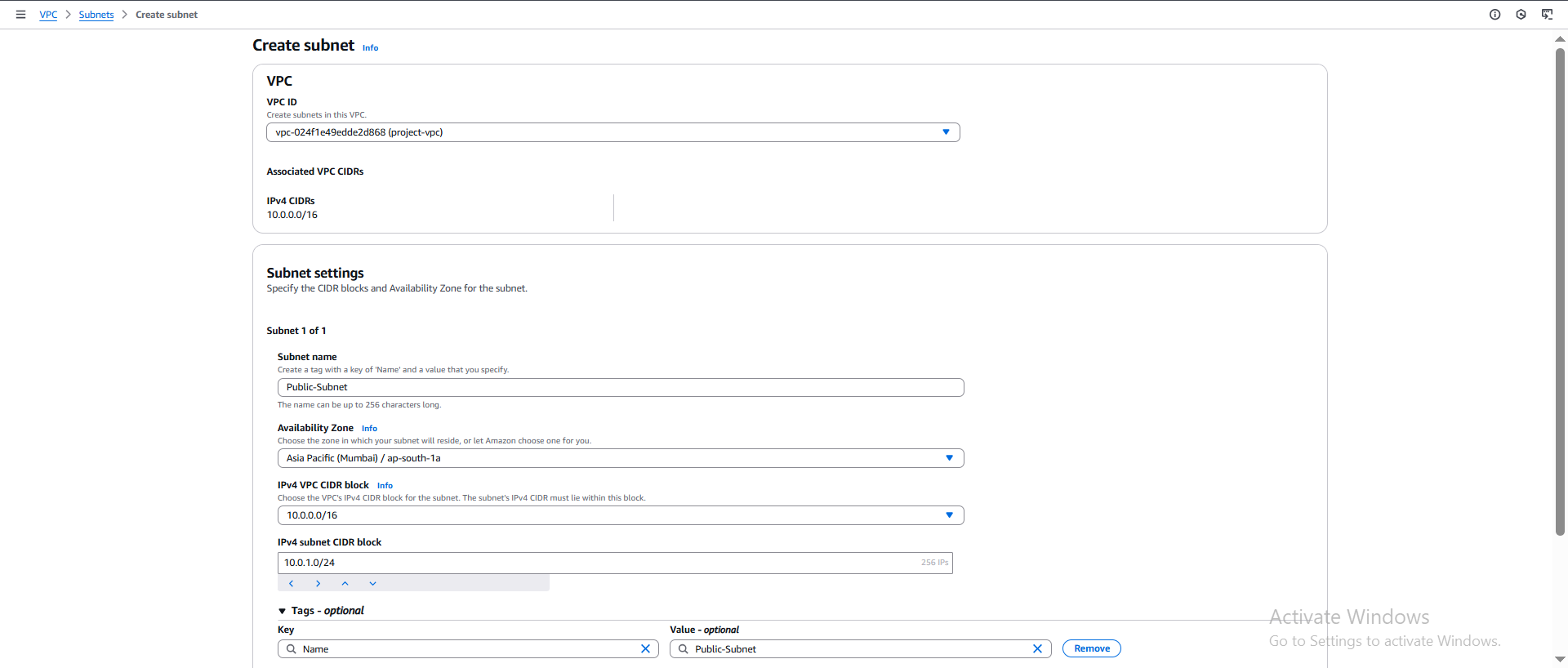
AWS Resources Overview

|  |  |
| --- | --- |
| Resource | Description |
| VPC | Custom VPC with CIDR 10.0.0.0/16 |
| IGW | Internet Gateway |
| NAT Gateway | Enables internet access for private subnet |
| Subnets | Public (10.0.1.0/24) & Private (10.0.2.0/24) |
| Route Tables | Separate route tables for public and private |
| Bastion Host | EC2 instance in public subnet for SSH access |
| Backend EC2 | EC2 instance in private subnet |
| Security Groups | SSH rules for Bastion and Backend EC2 |

**Step-by-Step Instructions**

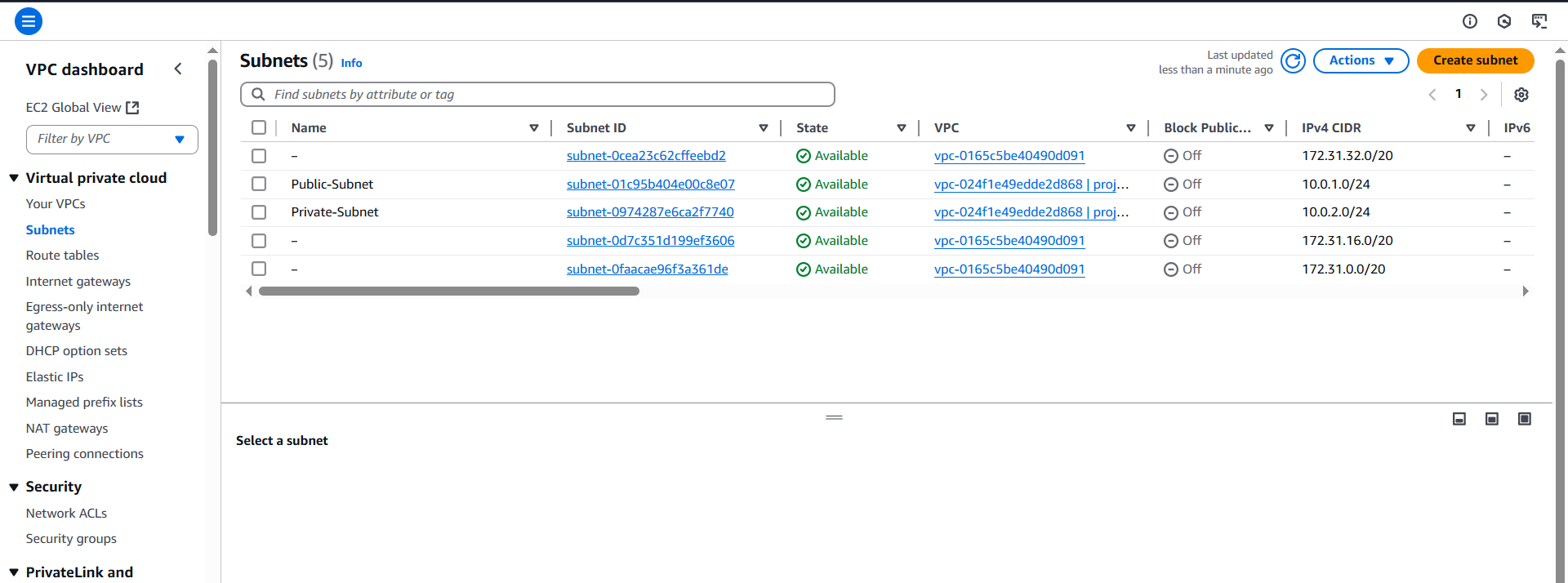
**Step 1: Create a VPC**

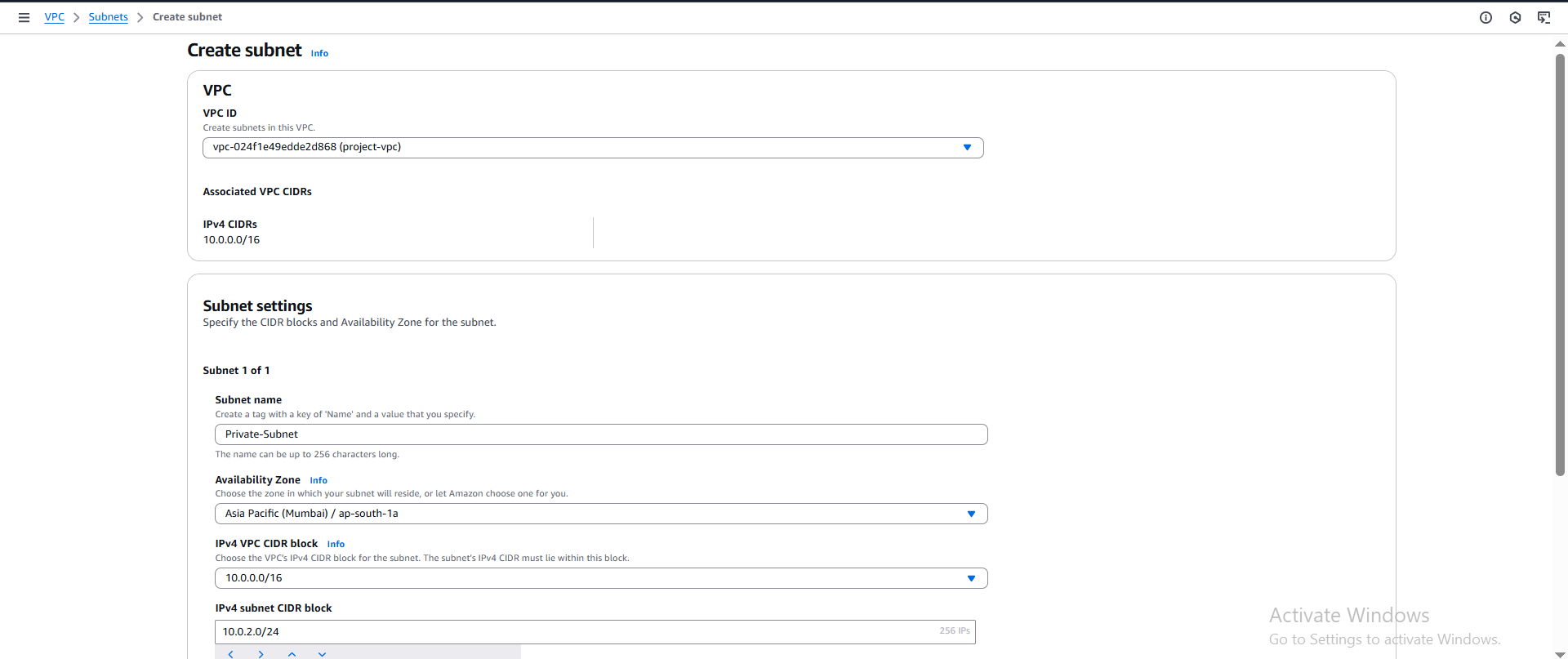
* Go to VPC Dashboard → Create VPC
* CIDR block: 10.0.0.0/16
* Enable DNS hostnames



**Step 2: Create Subnets**

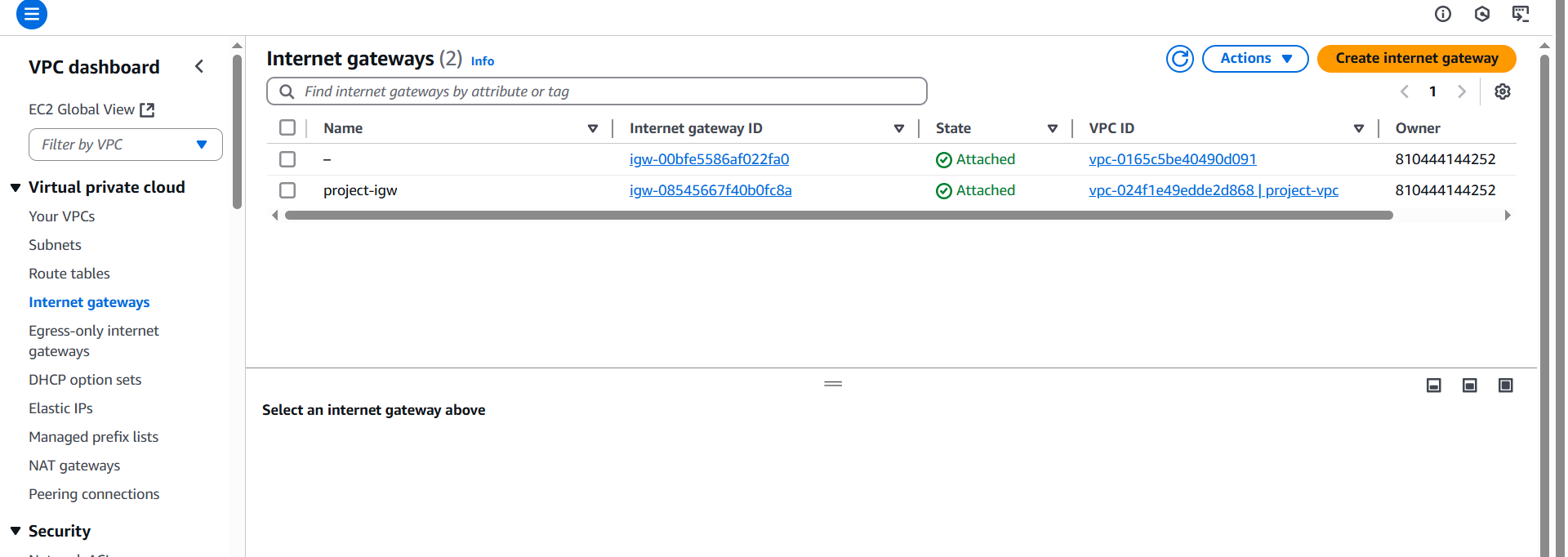
* Public Subnet: 10.0.1.0/24 (us-east-1a)
* Private Subnet: 10.0.2.0/24 (us-east-1a)

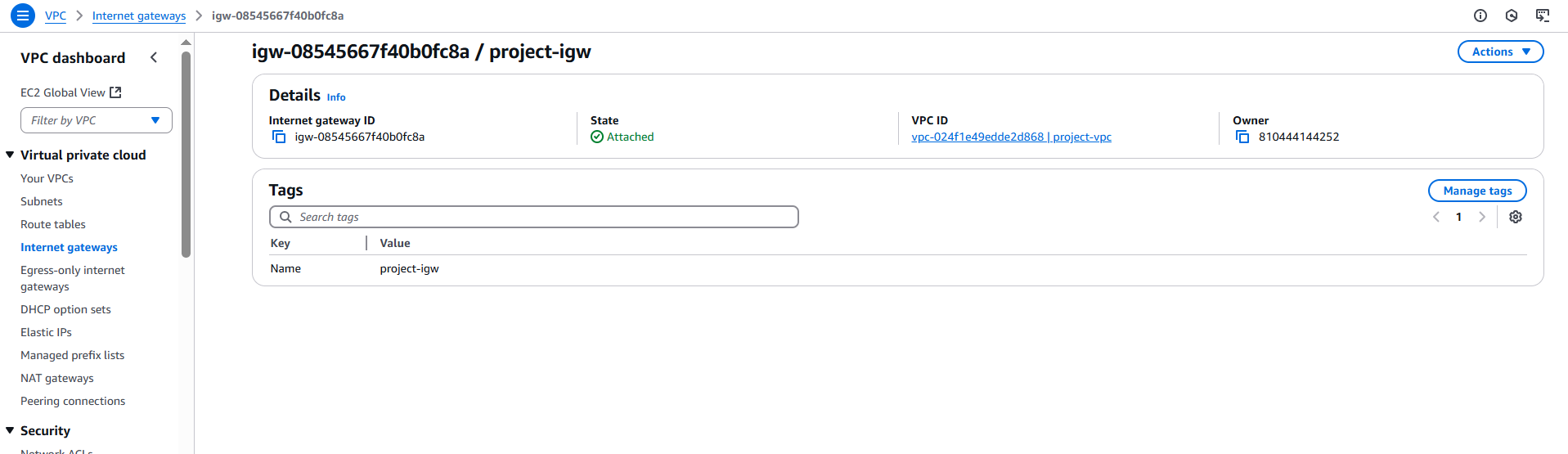




**Step 3: Create and Attach Internet Gateway**

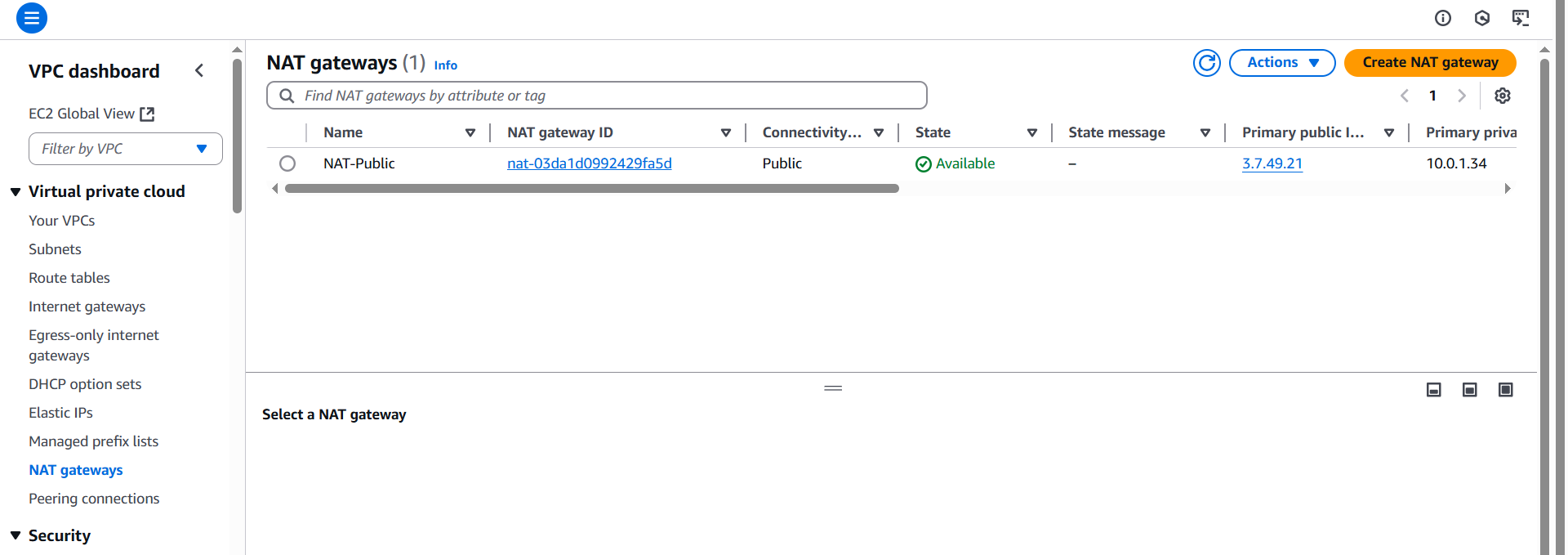
* Create an IGW
* Attach IGW to the VPC

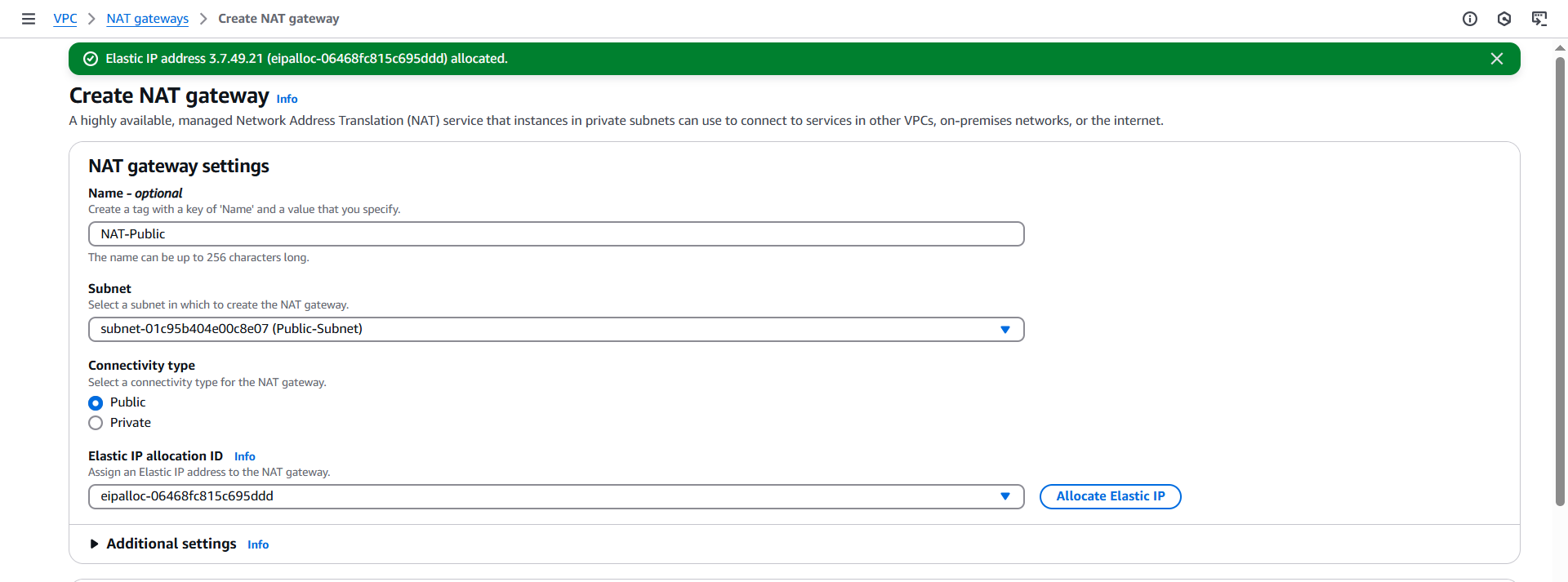




**Step 4: Create NAT Gateway**

* Allocate an Elastic IP
* Create NAT Gateway in the Public Subnet
* Assign the Elastic IP
* Wait for NAT Gateway to become available





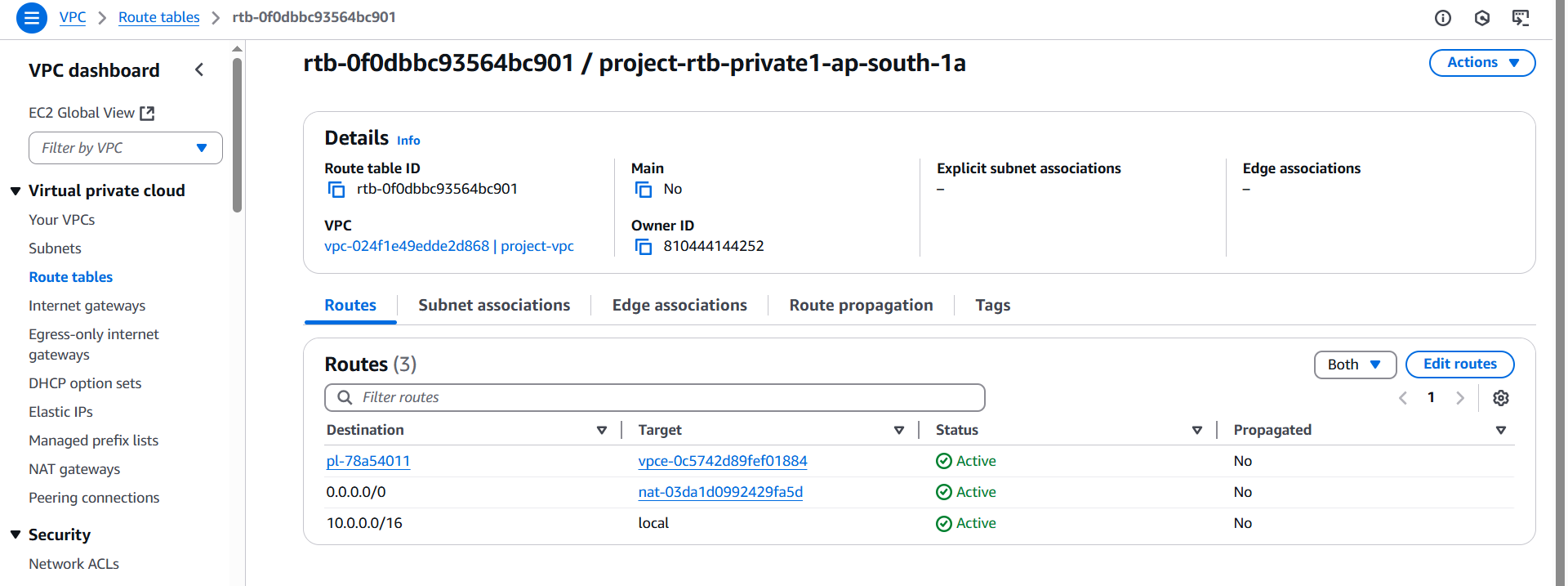
**Step 5: Create Route Tables**

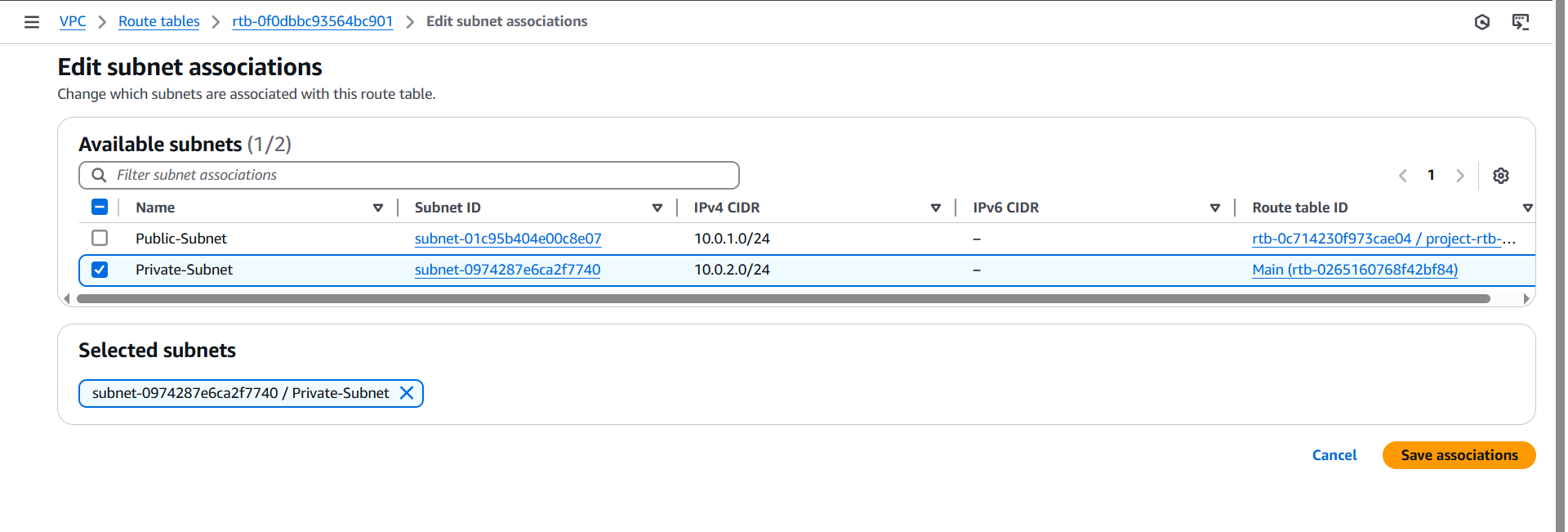
* Public Route Table: Associate with Public Subnet

1. Add route: 0.0.0.0/0 → IGW

* Private Route Table: Associate with Private Subnet

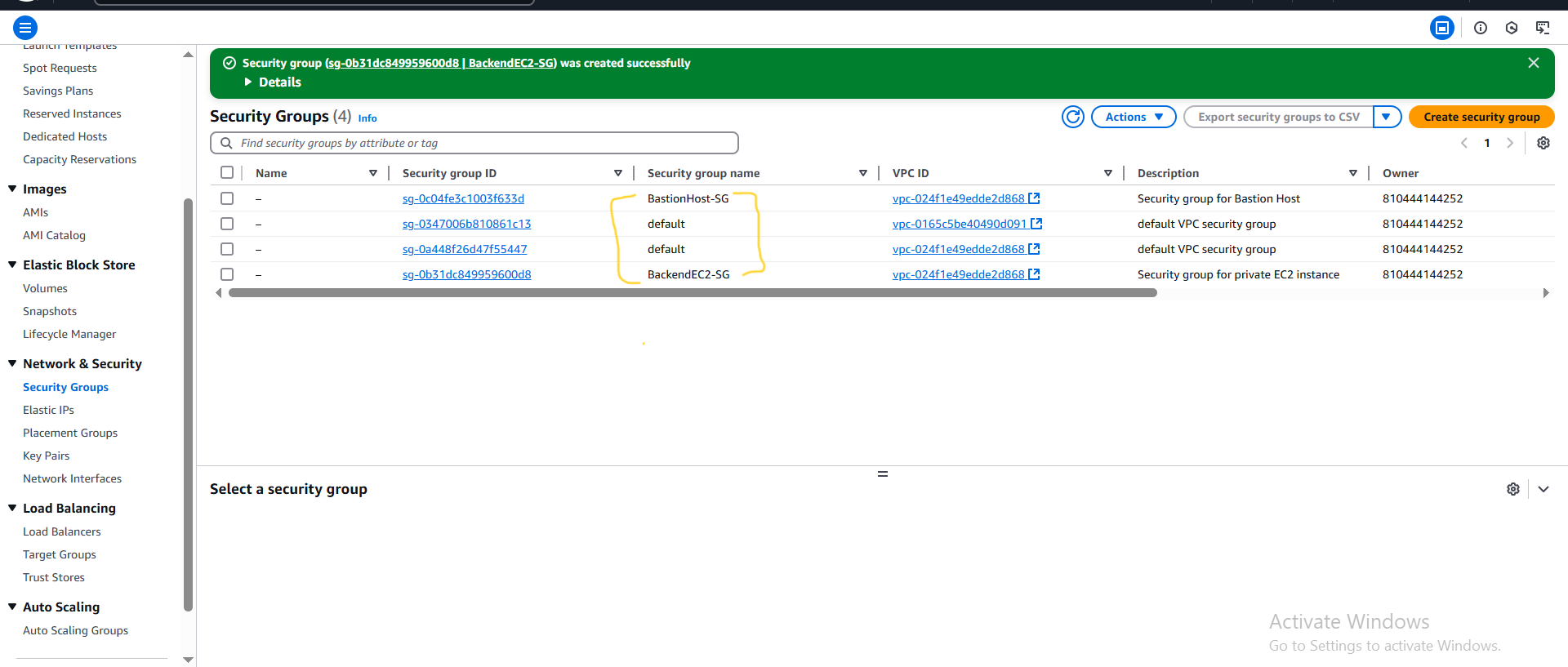
1. Add route: 0.0.0.0/0 → NAT Gateway

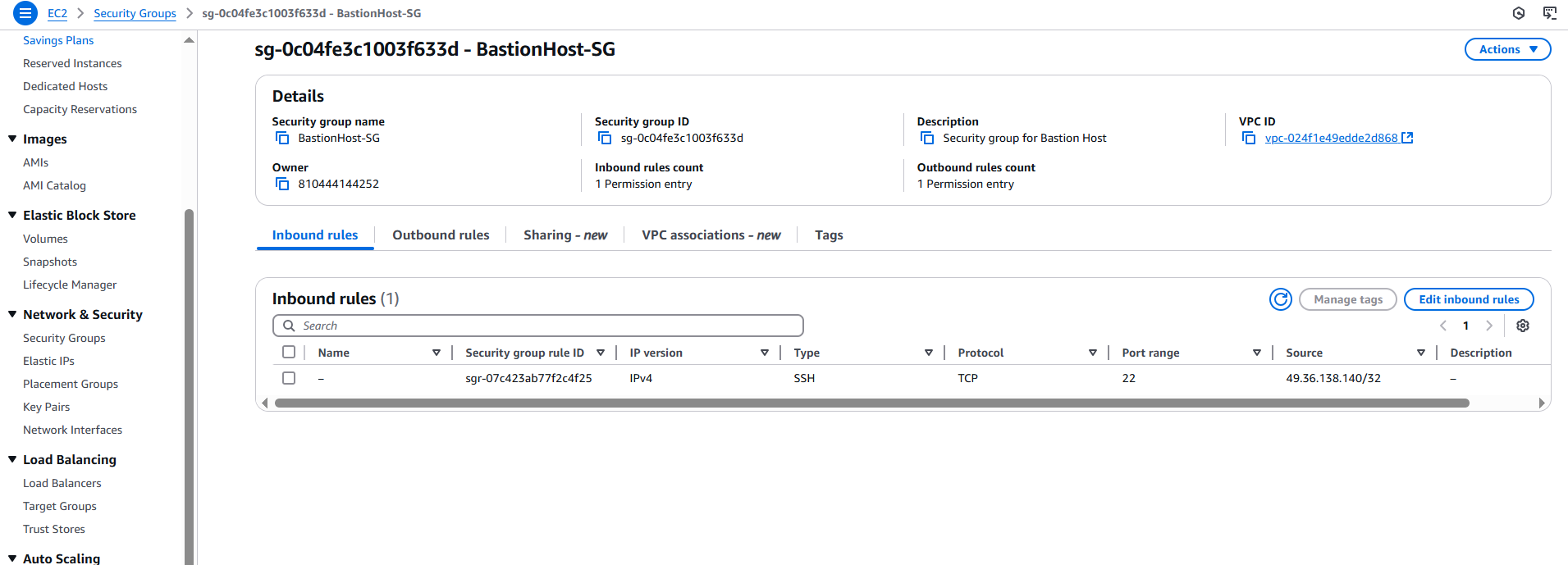


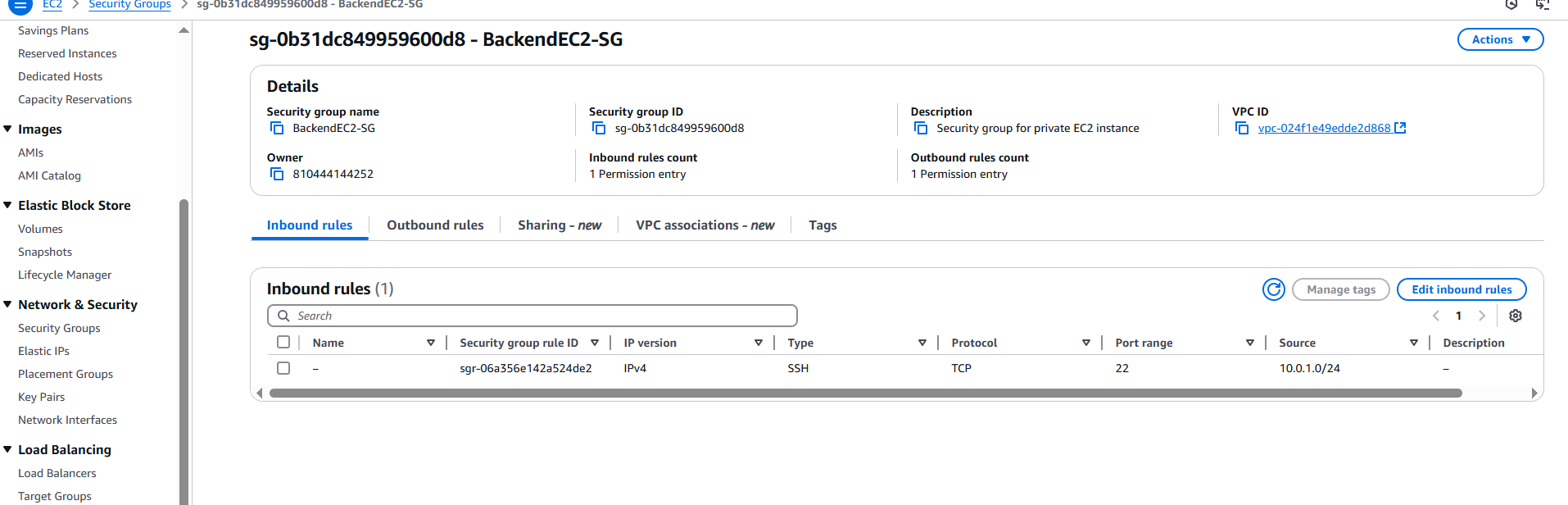


**Step 6: Configure Security Groups**

* Bastion Host SG - Inbound: SSH (22) from your IP (x.x.x.x/32)
* Backend EC2 SG - Inbound: SSH (22) from Bastion subnet (10.0.1.0/24)
* Outbound: Allow all (both SGs)

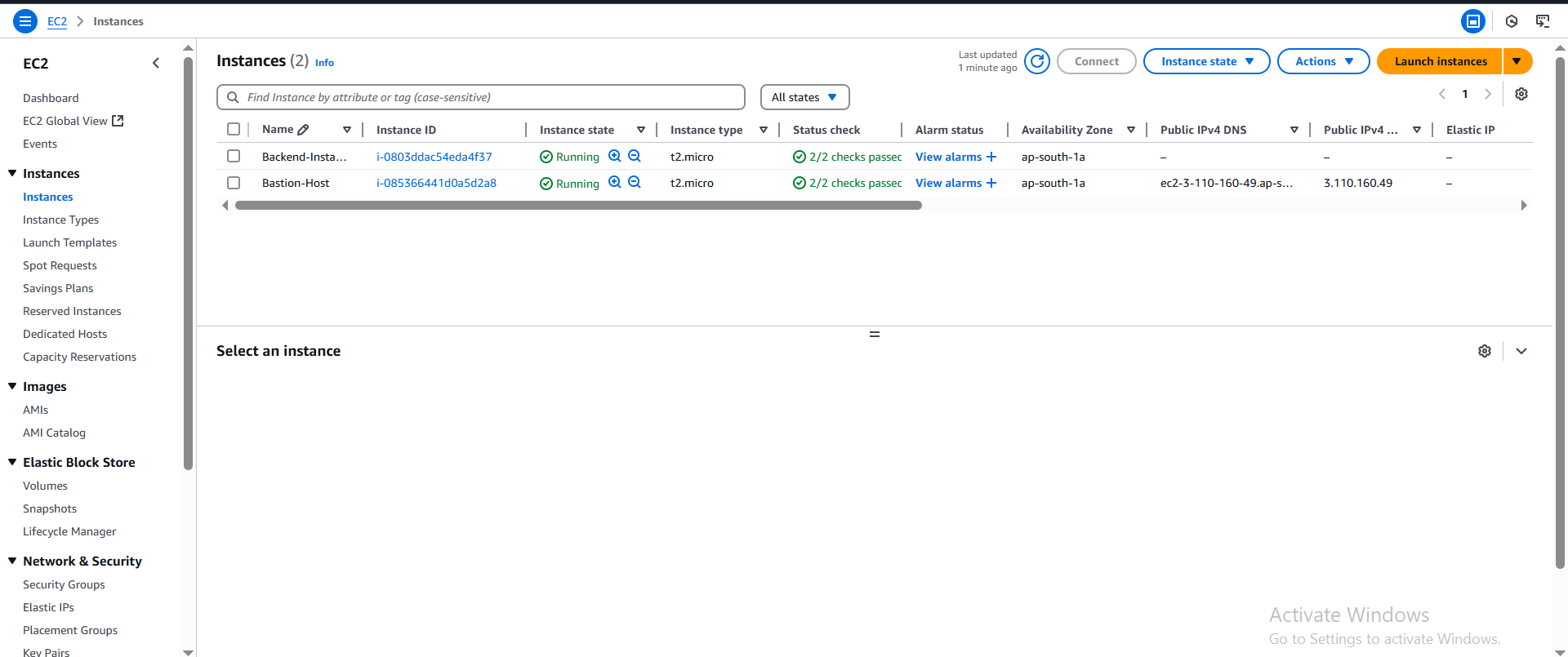


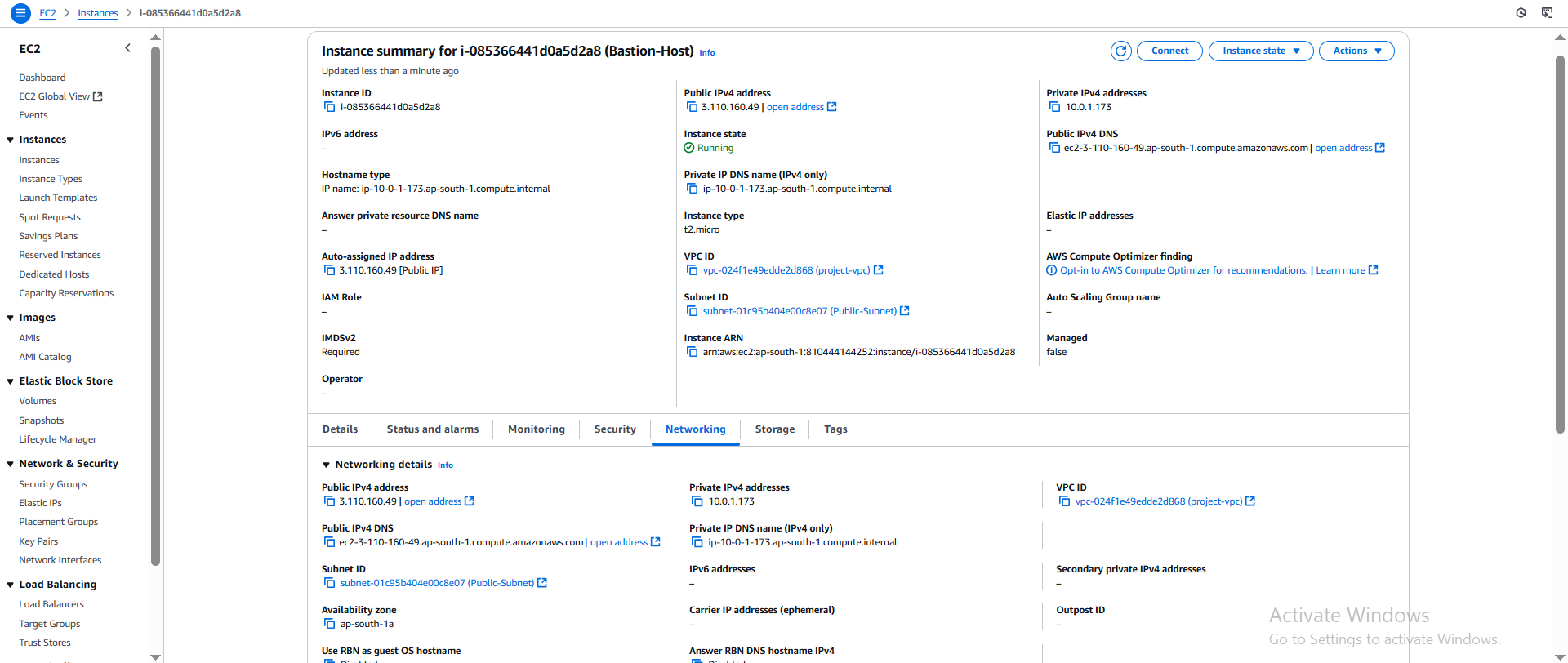


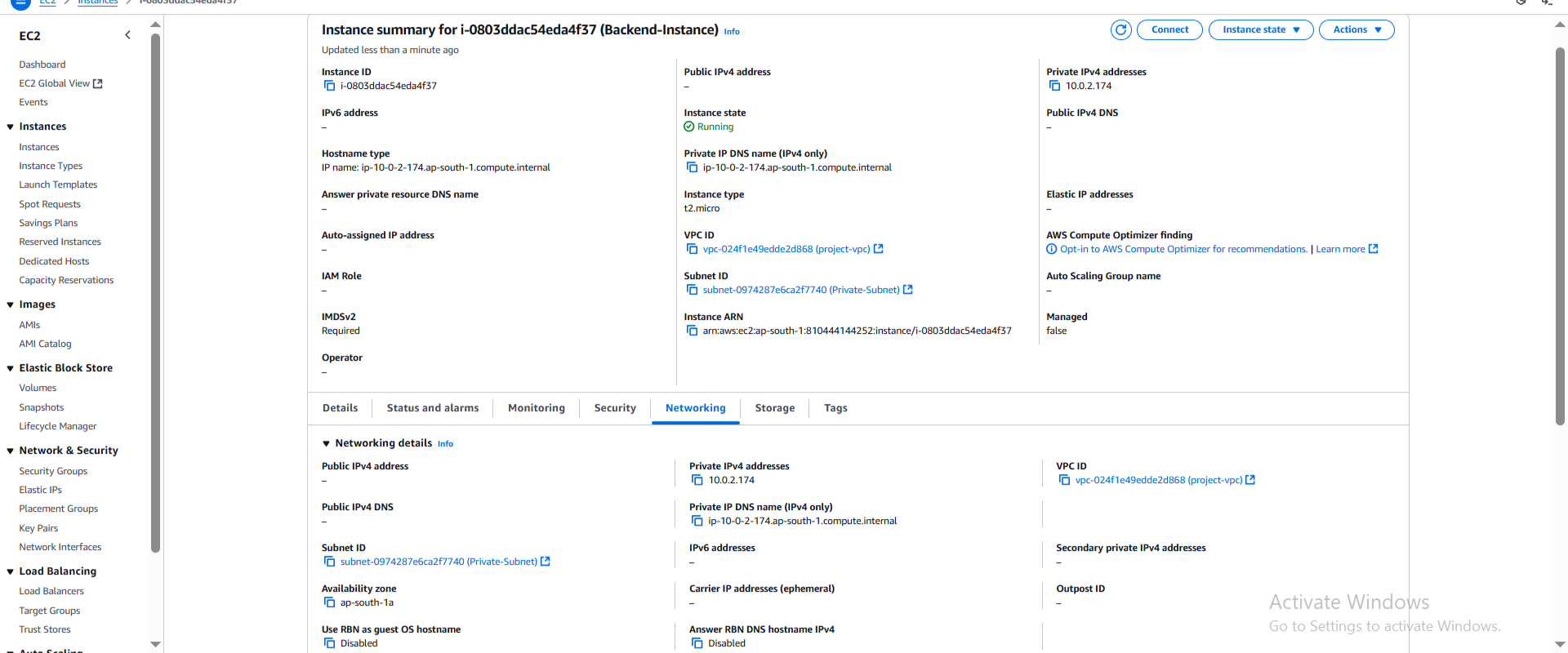


**Step 7: Launch EC2 Instances**

* Bastion Host: Public Subnet, Bastion SG, Key Pair
* Backend EC2: Private Subnet, Backend SG, Same Key Pair





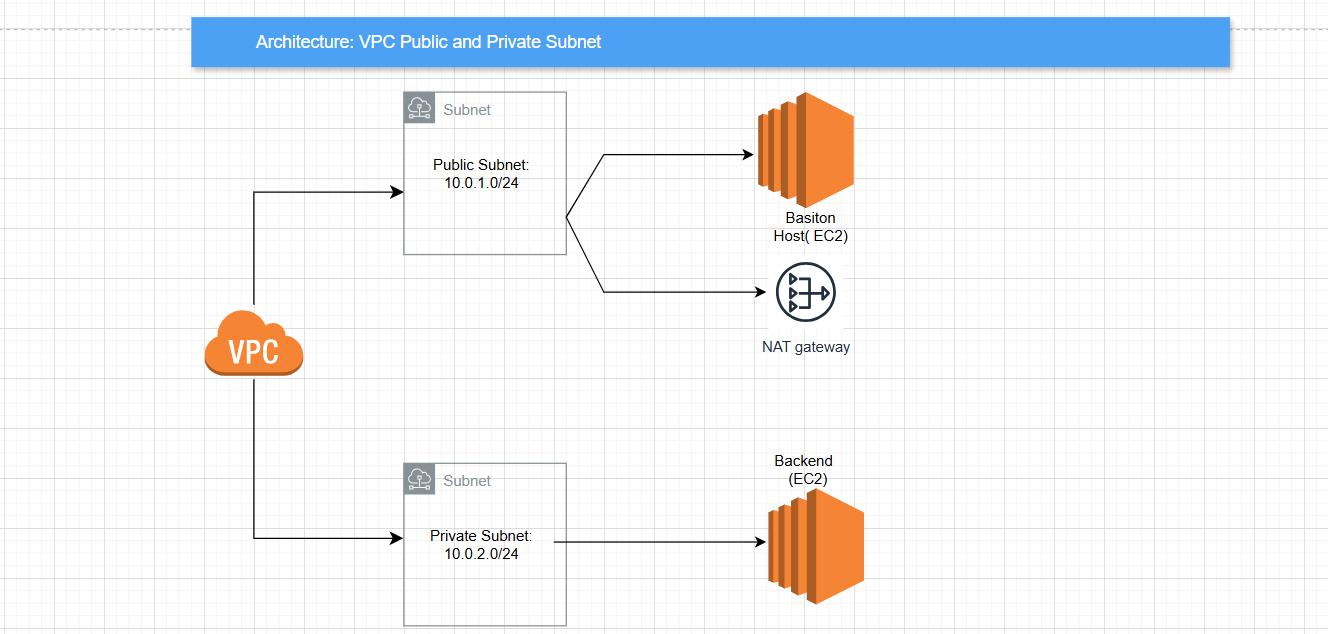


**Step 8: Validation Steps**

* SSH to Bastion: ssh -i my-key.pem ec2-user@<bastion-public-ip>
* SSH from Bastion to Private EC2: ssh -i my-key.pem ec2-user@<private-ip>
* Test Internet from Private EC2: ping google.com, sudo apt update -y

**Architecture Diagram**

VPC: 10.0.0.0/16  
├── Public Subnet: 10.0.1.0/24  
│ ├── Bastion Host (EC2)  
│ └── NAT Gateway  
└── Private Subnet: 10.0.2.0/24  
 └── Backend EC2



**Conclusion**

The setup described in this document creates a secure, logically separated AWS network architecture that enables safe SSH access to private EC2 instances and allows them internet access via a NAT Gateway.