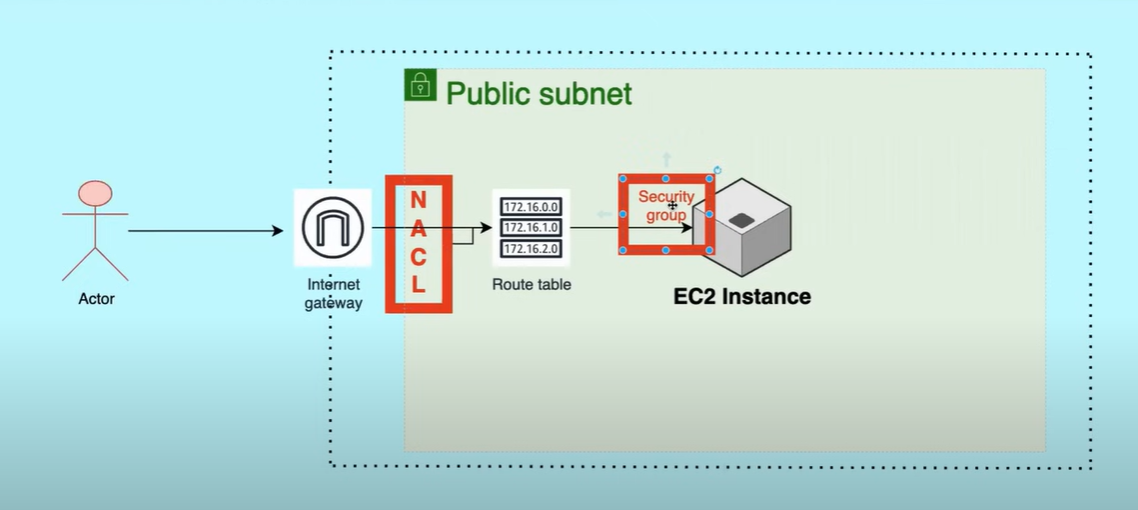
* 🚀 AWS Public Subnet Setup with EC2, VPC, Route Table, NACL, and Security Group

1. This project demonstrates the creation of a public subnet within an AWS Virtual Private Cloud (VPC), including configuration of essential components such as Internet Gateway, Route Table, Network Access Control List (NACL), Security Group, and EC2 instance deployment. It serves as a foundational exercise in cloud networking and infrastructure provisioning.



1. Create a VPC

# AWS Console Navigation: VPC > Create VPC VPC Name: DevOps-VPC IPv4 CIDR Block: 172.16.0.0/16 Tenancy: Default

1. Create a Public Subnet

# AWS Console Navigation: Subnets > Create Subnet Subnet Name: Public-Subnet-A VPC: DevOps-VPC Availability Zone: ap-south-1a IPv4 CIDR Block: 172.16.1.0/24

1. Create and Attach an Internet Gateway

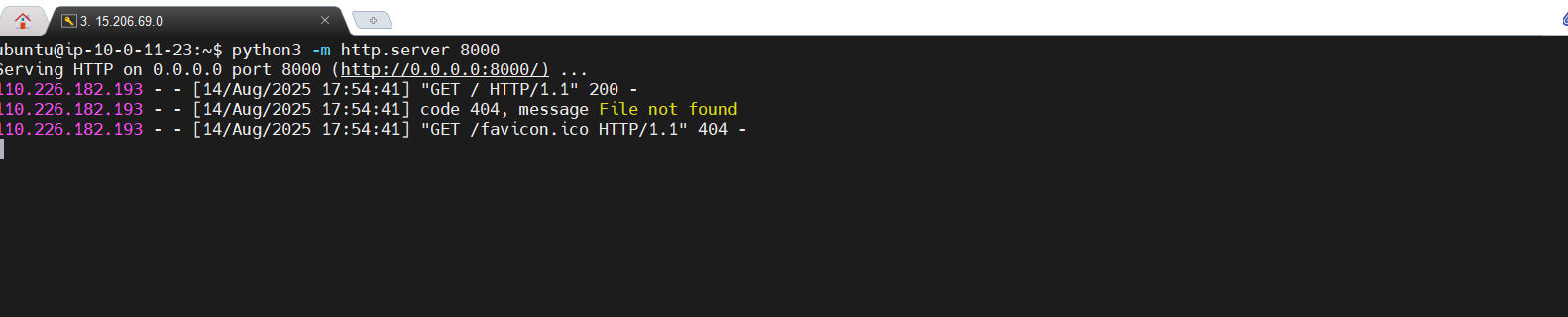
# AWS Console Navigation: Internet Gateways > Create Name: DevOps-IGW Attach to VPC: DevOps-VPC

1. Configure Route Table

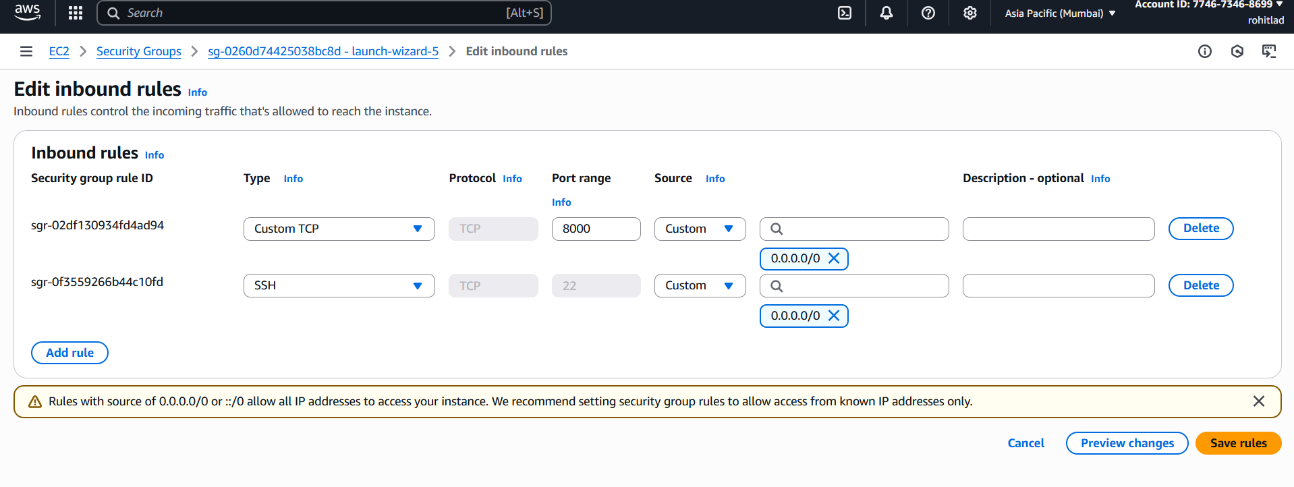
# AWS Console Navigation: Network ACLs > Create Name: Public-NACL VPC: DevOps-VPC # Inbound Rules Allow HTTP (80), HTTPS (443), SSH (22), and ephemeral ports (1024–65535) # Outbound Rules Allow all traffic (0.0.0.0/0) # Associate with Subnet Subnet: Public-Subnet-A

1. Launch EC2 Instance

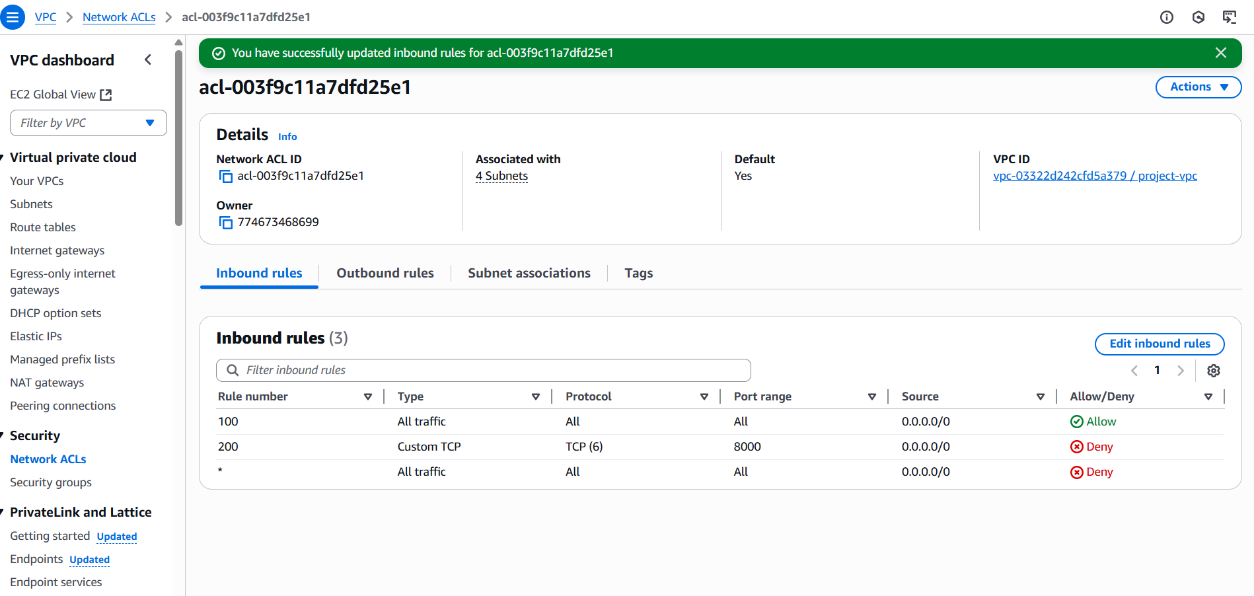
# AWS Console Navigation: EC2 > Launch Instance AMI: Amazon Linux 2 Instance Type: t2.micro Network: DevOps-VPC Subnet: Public-Subnet-A Auto-assign Public IP: Enabled # Security Group Inbound Rules: Allow SSH (22), HTTP (80), HTTPS (443) Outbound Rules: Allow all # Key Pair Create or use existing for SSH access

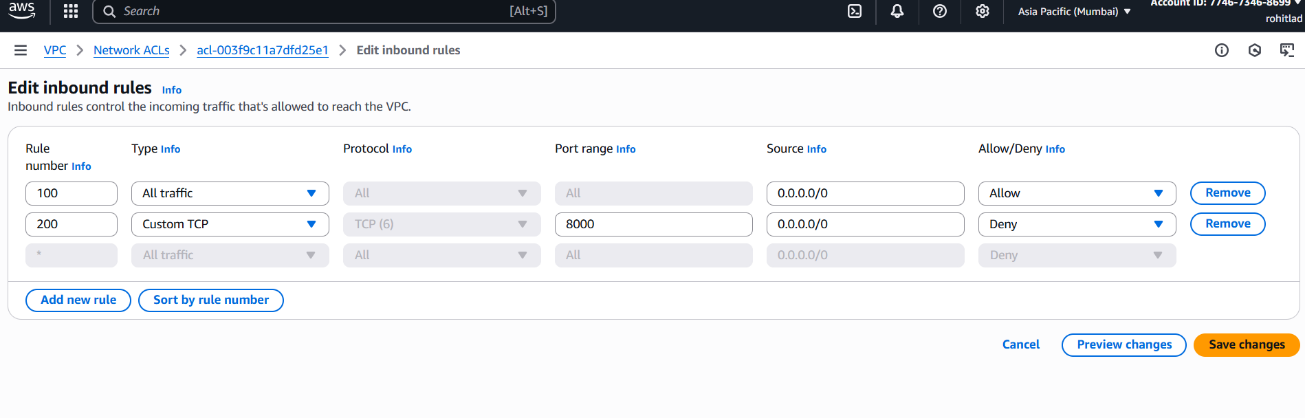


1. Change the Inbound rules in Security Group and give a port 8080 to connect with the IP address



1. NACL follows a basic ascending inbound rule .





✅ Outcomes

• Successfully provisioned a public subnet with secure access.

• Deployed an EC2 instance accessible via the internet.

• Configured NACL and Security Groups for layered security.

• Demonstrated understanding of AWS networking fundamentals.