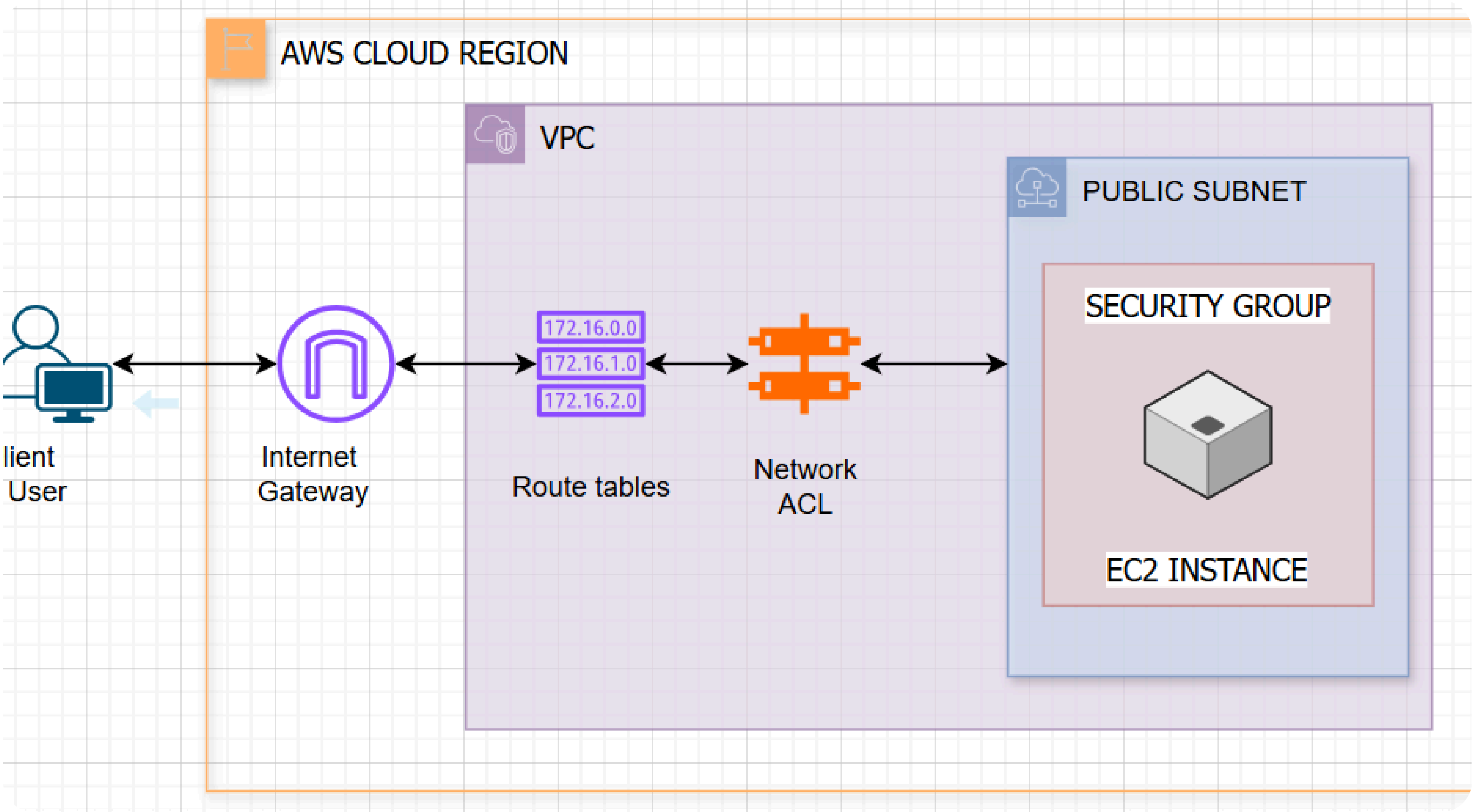
# VPC TRAFFIC FLOW AND SECURITY



MATHEW OLUWASEUN ADELOWO

linkedin.com/in/adelowomathew

github.com/Seun-d-creator/Aws

## Project Overview

In this step, i will be building a Route Table, Access control list (ACL) and security groups as a continuation of my network project.

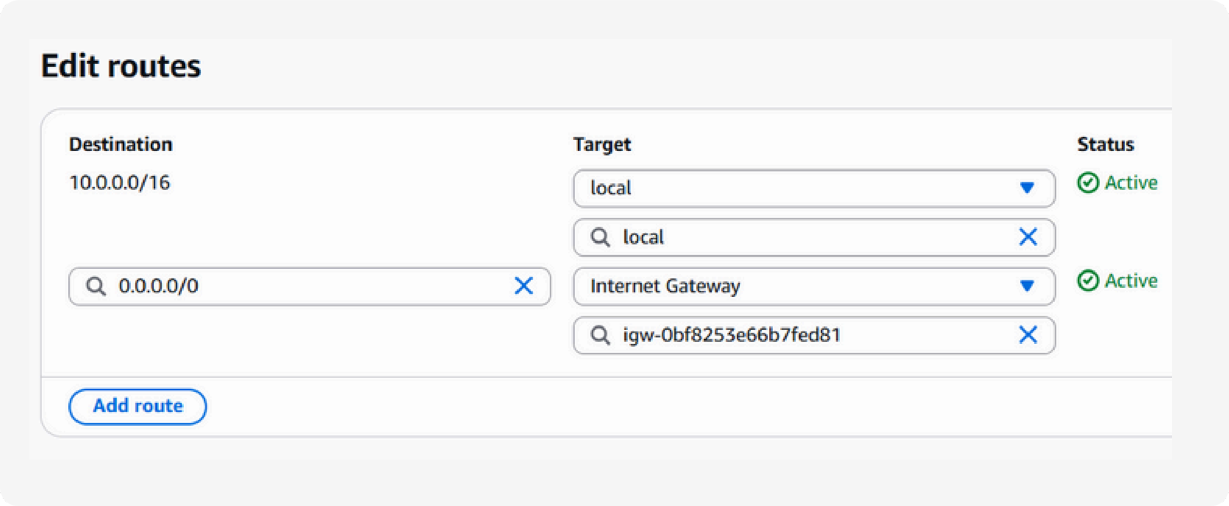
## What Is Route Table ?

- A route table is a set of rules (routes) that determine how network traffic is directed within a Virtual Private Cloud (VPC) or between network.

- Route tables are needed to make a subnet public because a subnet does not have a route to an internet gateway in order to be considered public. The route table is the only way to establish connection

- A route table consist of two routes, which destination and target. The destination is the range of IP addresses that traffic in my VPC is trying to reach while the target is the road/path that the traffic will have to take to get to its destination.

- The route in my route table that direct internet bound traffic to my internet gateway had a destination of 0.0.0.0/0 and a target of Proj IG (internet gateway)

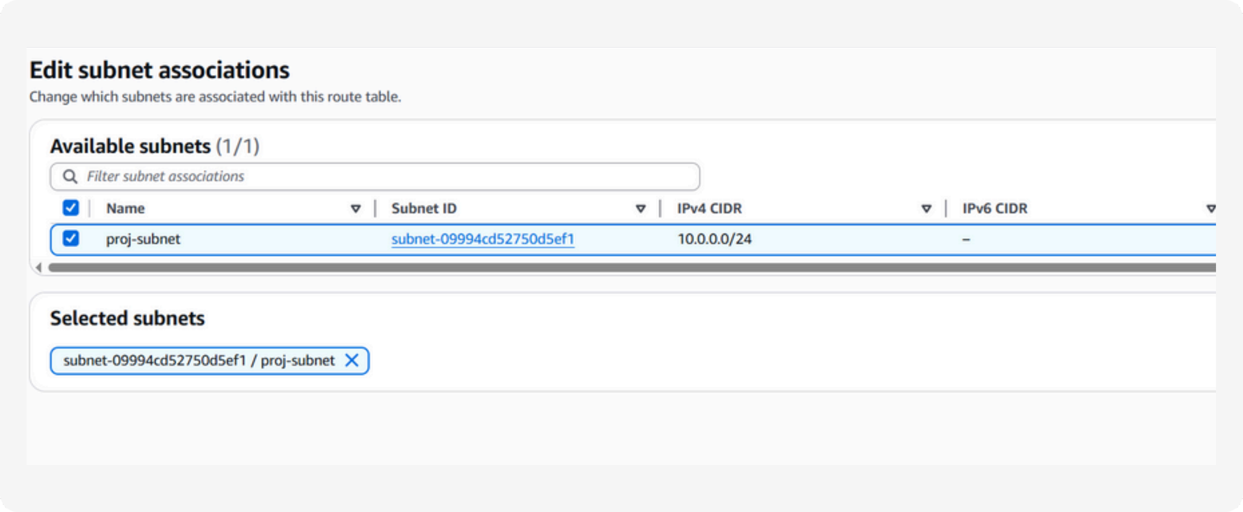


Edit routes

| Destination | Target | Status |
|---|---|---|
| 10.0.0.0/16 | local<br>local | ✓ Active |
| 0.0.0.0/0 | Internet Gateway<br>igw-0bf8253e66b7fed81 | ✓ Active |

The subnet was created without explicit association, meaning it hasn’t been linked to a custom route table. As a result, it is automatically associated with the main route table created by AWS.

i edited the route table subnet association and made an association with my subnet in other for my subnet to be consider public



Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/1)

| ☑ | Name | Subnet ID | IPv4 CIDR | IPv6 CIDR |
|---|---|---|---|---|
| ☑ | proj-subnet | subnet-09994cd52750d5ef1 | 10.0.0.0/24 | – |

Selected subnets

subnet-09994cd52750d5ef1 / proj-subnet

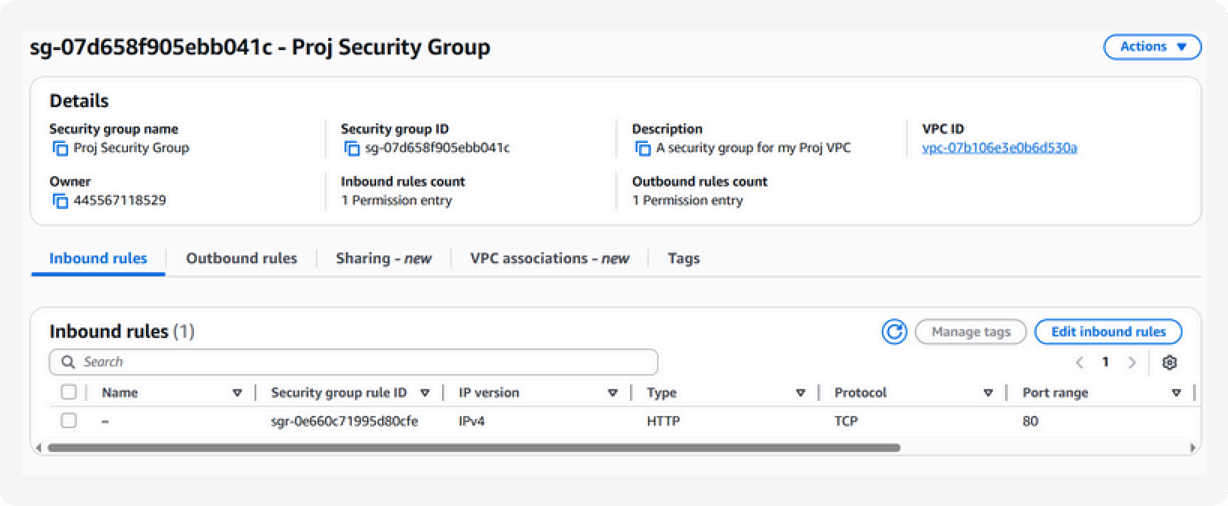
# What Is Security group ?

- A Security Group is a virtual firewall that is used to control inbound and outbound traffic to individual resources, such as EC2 instances, databases or load balancers.

- Security Group controls traffic flow using two types of rules
  - Inbound rules define which incoming traffic (based on IP, port, or protocol) is permitted to access a resource within a security group.
  - Outbound rules are a type of rule that monitor or restrict the traffic leaving a resource to the internet or other services e.g web app requesting data from public source

- By default, an outbound allows all outbound traffic

- I also configured an inbound rule that allows all inbound HTTP traffic



sg-07d658f905ebb041c - Proj Security Group

Details

|  |  |  |  |
|---|---|---|---|
| Security group name<br>Proj Security Group | Security group ID<br>sg-07d658f905ebb041c | Description<br>A security group for my Proj VPC | VPC ID<br>vpc-07b106e3e0b6d530a |
| Owner<br>445567118529 | Inbound rules count<br>1 Permission entry | Outbound rules count<br>1 Permission entry |  |

Inbound rules (1)

| □ | Name | Security group rule ID | IP version | Type | Protocol | Port range |
|---|---|---|---|---|---|---|
| □ | – | sgr-0e660c71995d80cfe | IPv4 | HTTP | TCP | 80 |

# Network Access Control List

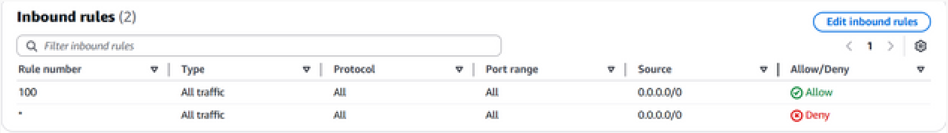
- Network ACL controls inbound and outbound traffic to and from subnets using rule-based filters like IP, port, and protocol.

- The difference between the Security group and ACL is their scope. Security group secures my network at the resource level(every single resources in my VPC is associated to the security group) while the network ACL secures my network at subnet level.

- Having both network ACL and security Group is a good practice because it create dual layer of security that makes sure our resources is secure

- Similar to security groups, network Acl use inbound and outbound rules:
  - A default NACL allows inbound rule is set up to allow all incoming traffic
  - A default NACL outbound rules is set up to allow all outgoing traffic
  - In contrast custom ACL's inbound and outbound rules are automatically set to deny all incoming and outgoing traffic

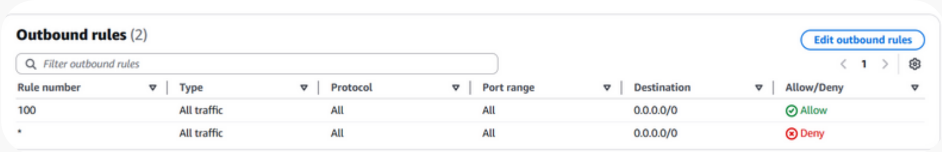
My network Acl inbound rule



**Inbound rules** (2)

| Rule number | Type | Protocol | Port range | Source | Allow/Deny |
|---|---|---|---|---|---|
| 100 | All traffic | All | All | 0.0.0.0/0 | ✓ Allow |
| * | All traffic | All | All | 0.0.0.0/0 | ⊗ Deny |

My network Acl outbound rule



**Outbound rules** (2)

| Rule number | Type | Protocol | Port range | Destination | Allow/Deny |
|---|---|---|---|---|---|
| 100 | All traffic | All | All | 0.0.0.0/0 | ✓ Allow |
| * | All traffic | All | All | 0.0.0.0/0 | ⊗ Deny |