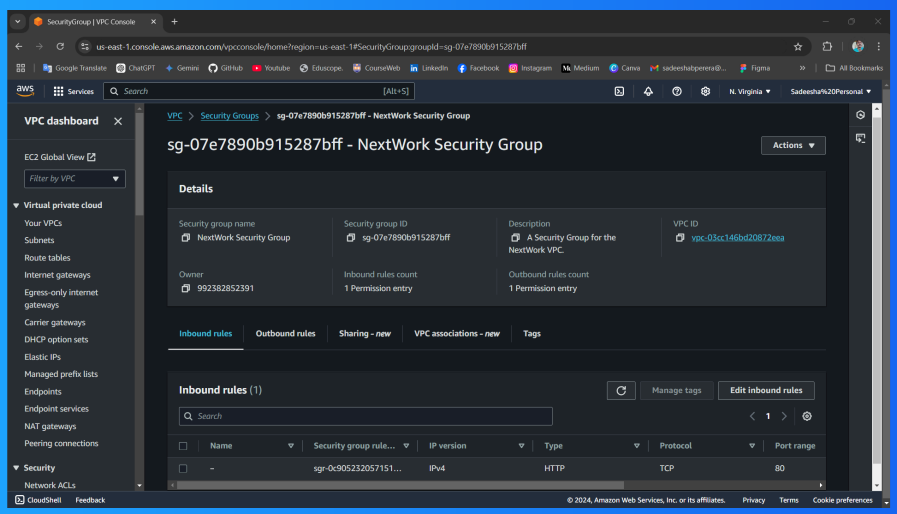
NextWork.org

# VPC Traffic Flow and Security

Sadeesha Perera



**Sadeesha Perera**
NextWork Student



# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is a service that lets you create a logically isolated section within the AWS cloud, providing you with complete control over your virtual network. It offers enhanced security, scalability, flexibility, and cost-effectiveness.

## How I used Amazon VPC in this project

To build a secure application, I used Amazon VPC to create a virtual network. This involves creating a VPC, defining public and private subnets, configuring route tables, and creating security groups.

## One thing I didn't expect in this project was...

How easy to enable security measurements in the AWS environment

## This project took me...

50 minutes

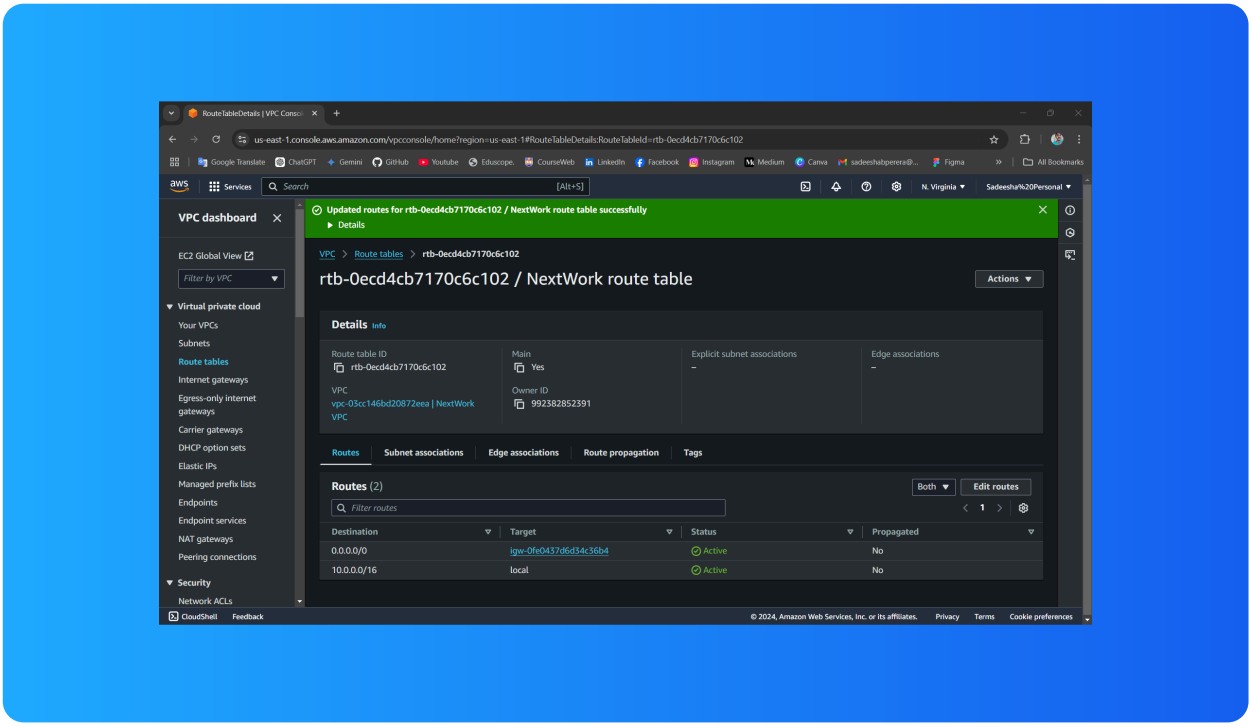
**Sadeesha Perera**
NextWork Student



# Route tables

Route tables are like a set of rules that determine how network traffic flows within your virtual network. Each subnet is associated with a route table, defining where specific IP traffic should be directed based on destination CIDR blo

Routes tables are needed to make a subnet public because it determines how network traffic from that subnet is routed. To make a subnet public, you need to associate it with a route table that contains a route pointing to an internet gateway.



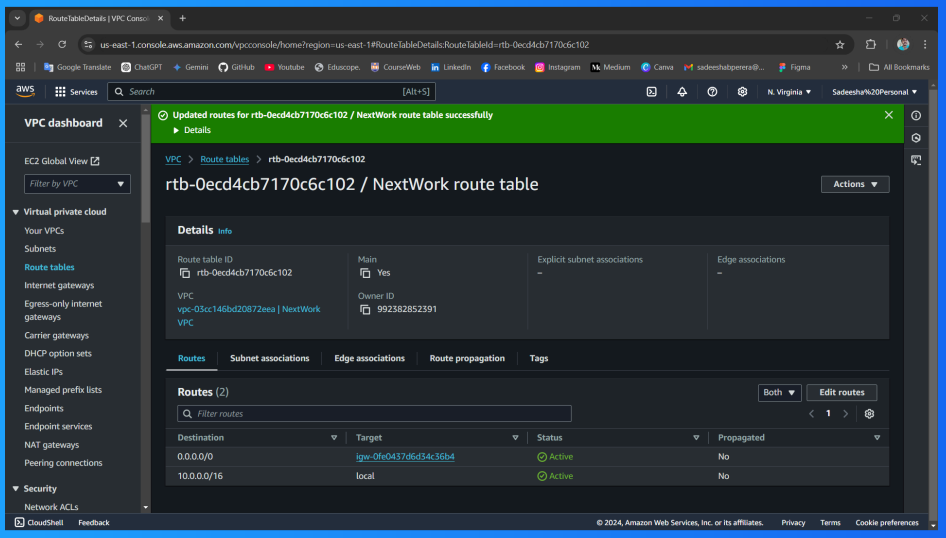
**Sadeesha Perera**
NextWork Student



# Route destination and target

A route in a route table consists of a destination and a target. The destination specifies the range of IP addresses the route applies to, while the target indicates where traffic matching that destination should be sent.

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of 0.0.0.0/0 and a target of igw-0fe534534b



**Sadeesha Perera**
NextWork Student



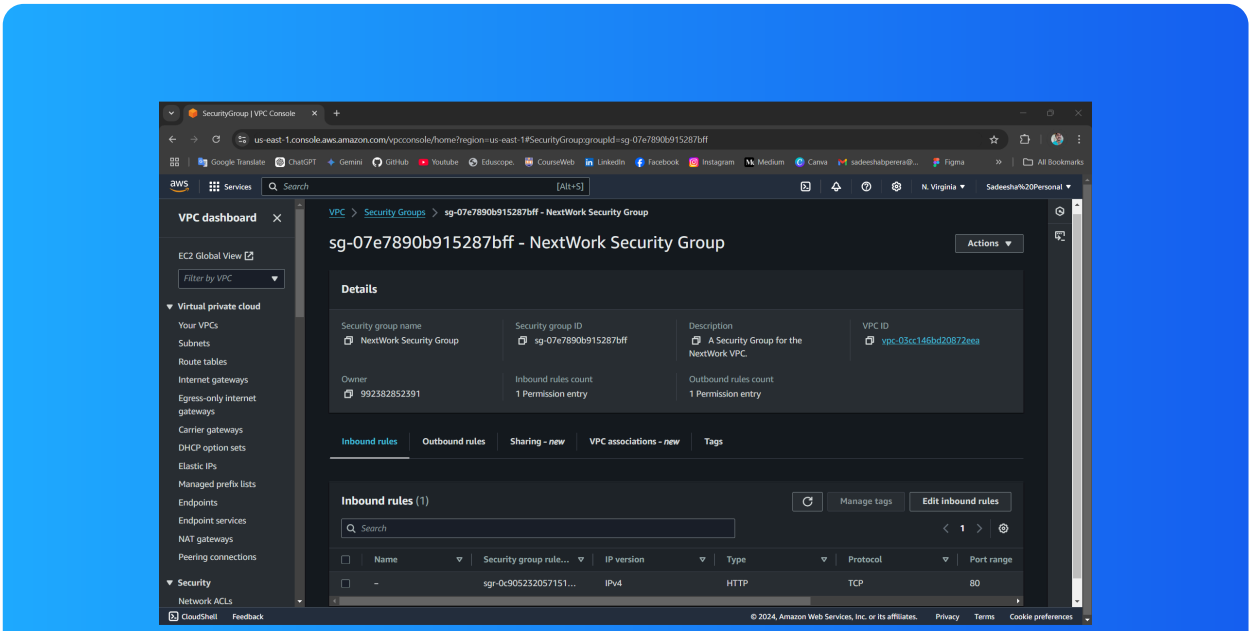
# Security groups

Security groups act as virtual firewalls for your EC2 instances, controlling both inbound and outbound traffic. They operate on a "deny all" principle, meaning that all traffic is blocked unless explicitly allowed by a specific rule.

## Inbound vs Outbound rules

An inbound rule in a security group defines the types of traffic allowed to enter an EC2 instance. It specifies the source IP address range, port range, and protocol for incoming traffic.

An outbound rule in a security group defines the types of traffic that an EC2 instance is allowed to send out. It specifies the destination IP address range, port range, and protocol for outgoing traffic.



**Sadeesha Perera**
NextWork Student



# Network ACLs

Network Access Control Lists (NACLs) are another layer of security for your VPC. They act as a firewall for traffic entering or leaving a subnet.Unlike security groups, which are associated with individual instances, NACLs are associated with subnets

## Security groups vs. network ACLs

Security groups and network ACLs are both used to control traffic within a VPC, but they differ in scope and operation. Security groups operate at the instance level, controlling traffic to and from individual EC2 instances.

**Sadeesha Perera**
NextWork Student

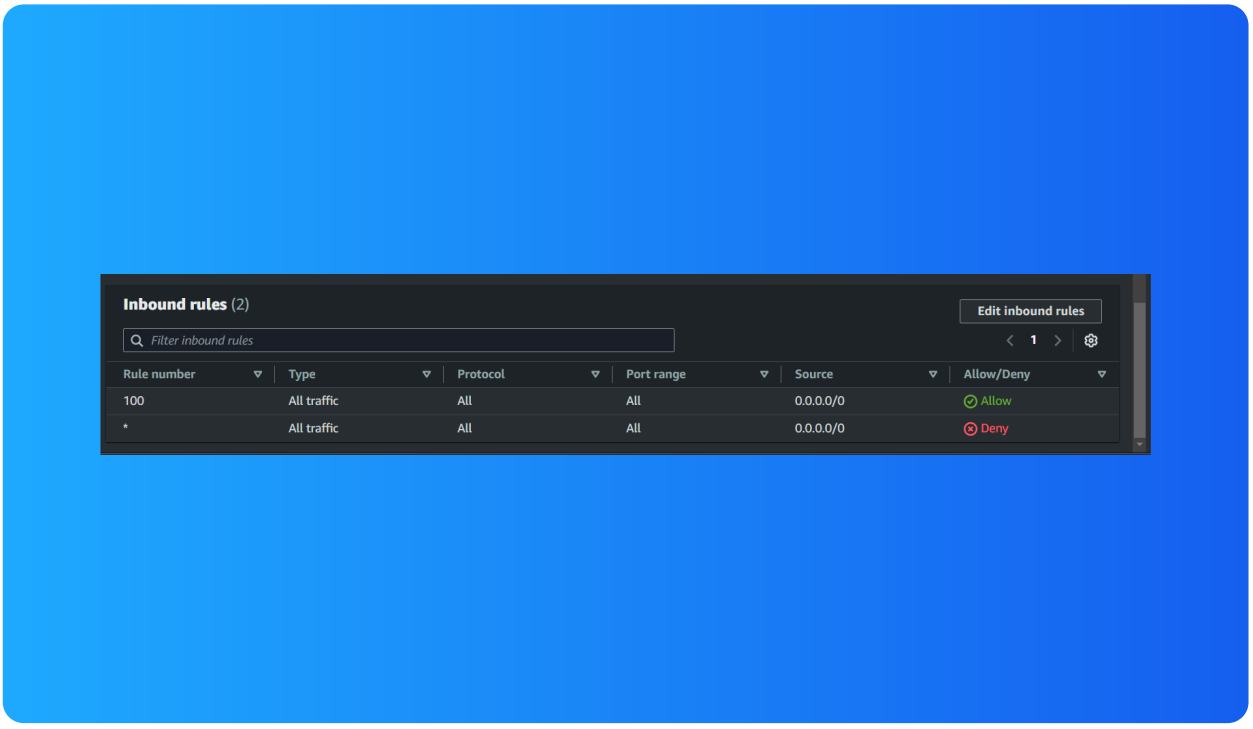


# Default vs Custom Network ACLs

## Similar to security groups, network ACLs use inbound and outbound rules

By default, network ACLs allow all inbound and outbound traffic. This means that unless you explicitly add rules to deny specific traffic, all traffic will be permitted.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny.



# Everyone should be in a job they love.

Check out nextwork.org for more projects