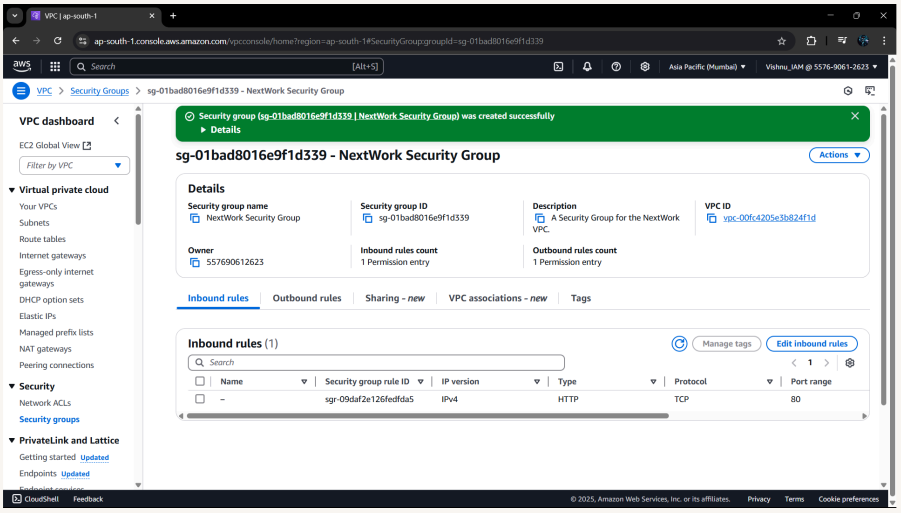
nextwork.org

VPC Traffic Flow and Security

V vishnu vardhan gurram



vishnu vardhan gurram
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private virtual network in AWS that lets you securely run and control your resources. It’s useful for managing network settings and protecting your data.

How I used Amazon VPC in this project

In today’s project, I used Amazon VPC to create a secure network with subnets, route tables, and an internet gateway. I also set up security groups to control instance traffic and network ACLs to protect the subnets.

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

One thing I didn’t expect was how much impact proper network and security settings have on making sure everything works smoothly and stays protected.

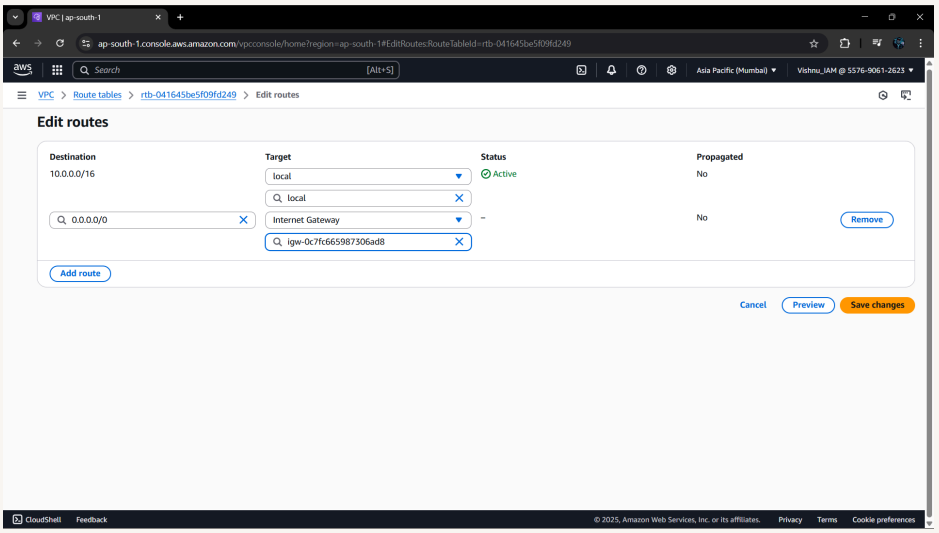
This project took me...

This project took me around 45 minutes to set up the VPC, subnets, route tables, internet gateway, and configure basic security groups and network ACLs.

Route tables

Route tables are a set of rules in a VPC that determine how network traffic is directed. They control the flow of traffic within the VPC and between the VPC and external networks like the internet.

Route tables are needed to make a subnet public because they define how traffic is routed. To make a subnet public, the route table must have a route that directs internet-bound traffic (0.0.0.0/0) to the internet gateway.

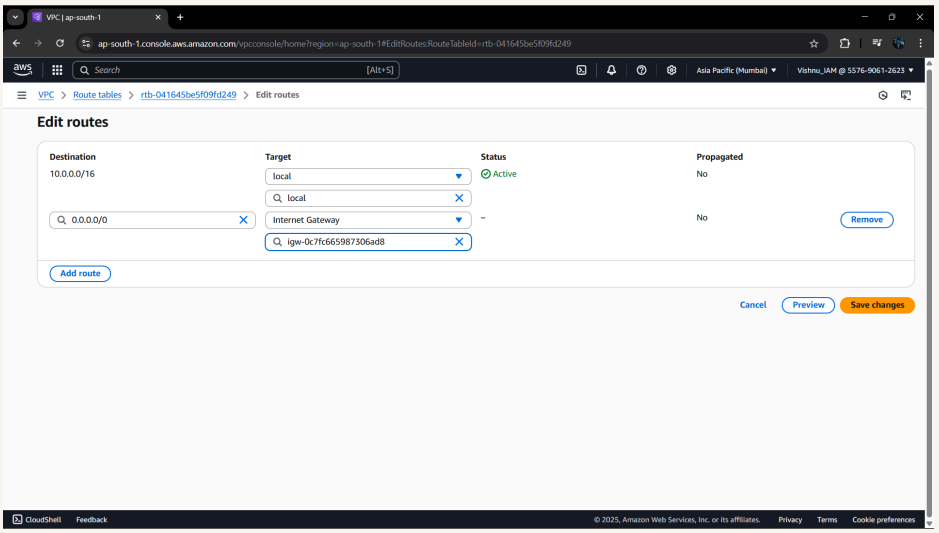


vishnu vardhan gurram
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the destination is the IP range the traffic is going to, and the target is where that traffic should be sent, such as an internet gateway, NAT gateway, or another subnet.

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 the internet gateway (igw-xxxxxxxx.



Security groups

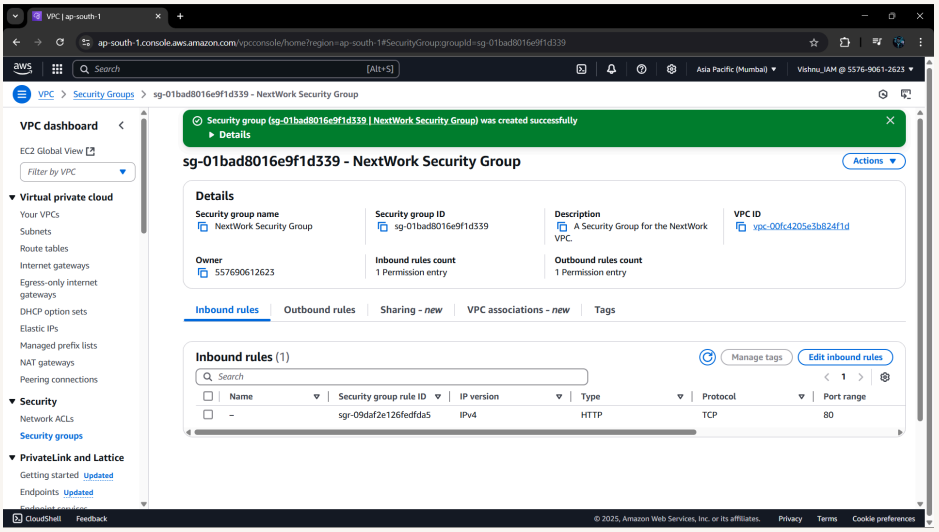
Security groups are virtual firewalls in AWS that control inbound and outbound traffic for resources like EC2 instances. They work at the instance level and allow you to define rules based on IP addresses, protocols, and ports.

Inbound vs Outbound rules

Inbound rules are settings in a security group that control the traffic allowed to enter your resource. I configured an inbound rule that allowed HTTP traffic (port 80) from anywhere so that my web server could be accessed publicly.

Outbound rules are settings in a security group that control the traffic allowed to leave your resource. By default, my security group's outbound rule allowed all traffic to any destination

vishnu vardhan gurram
NextWork Student



Network ACLs

Network ACLs are stateless firewalls at the subnet level in a VPC that control inbound and outbound traffic. They allow or deny traffic based on rules and apply to all resources within the associated subnet.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are stateful and apply to instances, while network ACLs are stateless and apply to subnets.

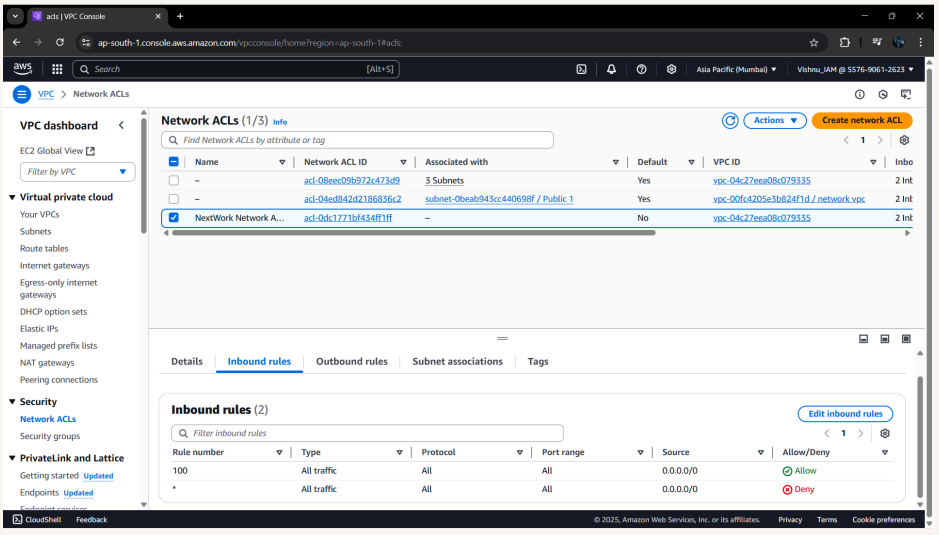
vishnu vardhan gurram
NextWork Student

Default vs Custom Network ACLs

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

By default, a network ACL's inbound and outbound rules will allow all traffic to pass through. This means no restrictions are applied unless you create specific rules to block or limit traffic for added security.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic by default, so you must create specific rules to allow or deny traffic based on IP addresses, protocols, and ports.



The place to learn & showcase your skills

Check out nextwork.org for more projects