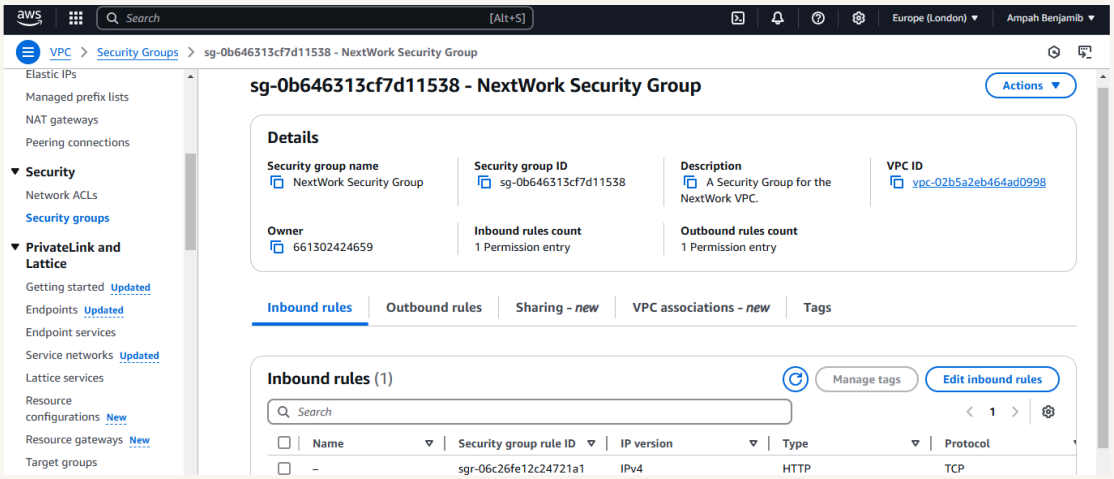
nextwork.org

VPC Traffic Flow and Security

AM ampahben3@gmail.com



AM
ampahben3@gmail.com
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private cloud network in AWS, giving control over IPs, subnets, routes, and security. It's useful for securing and managing resources in my project, ensuring efficient communication while restricting access as needed.

How I used Amazon VPC in this project

I used Amazon VPC in today's traffic flow project to manage network communication. I configured subnets, route tables, security groups, and network ACLs to control inbound and outbound traffic, ensuring secure and efficient data flow.

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

I didn't expect how network ACL (Access Control List) rules are evaluated in order. It required careful rule placement to avoid unintended traffic blocks, which impacted the expected flow until properly adjusted.

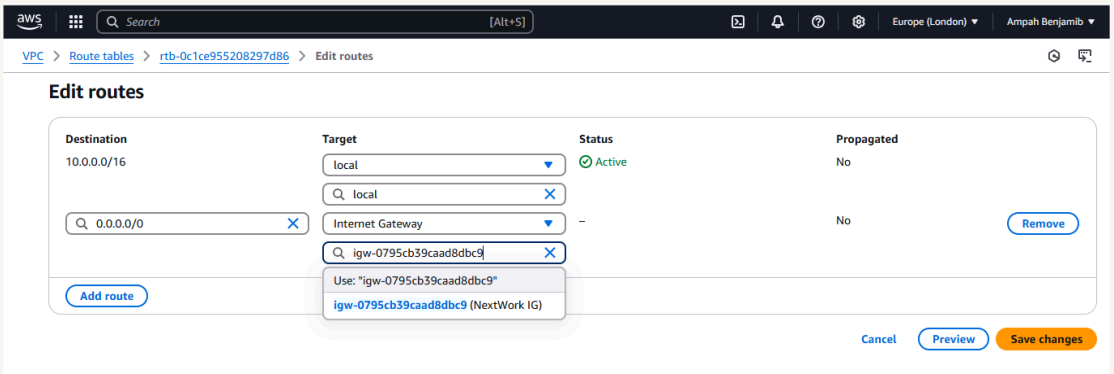
This project took me...

This project took me 1 hour since it was my first time adding security groups and network ACLs to my VPC(Virtual Private Cloud). Configuring them correctly required careful planning to ensure proper traffic flow.

Route tables

Route tables are a set of rules that determine where network traffic is directed based on destination IP addresses. They help route data within and between networks, ensuring packets reach their intended destination efficiently.

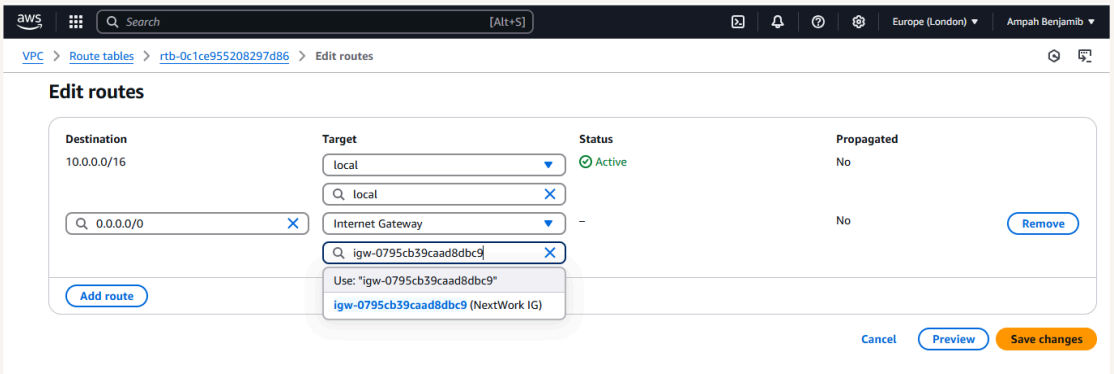
Route tables are needed to make a subnet public because they route traffic to an internet gateway (IGW), allowing external access. Without this route, the subnet cannot communicate with the internet, even if it has a public IP.



Route destination and target

Routes are defined by their destination and target, which mean the destination is the IP range of traffic, and the target is where that traffic is sent, such as an internet gateway, NAT gateway, or another network interface.

Routes are defined by their destination and target, which mean the destination is the traffic's IP range, and the target is where it's sent, like `0.0.0.0/0` for internet via IGW or `10.0.0.0/16` for internal VPC traffic.



AM
ampahben3@gmail.com
NextWork Student

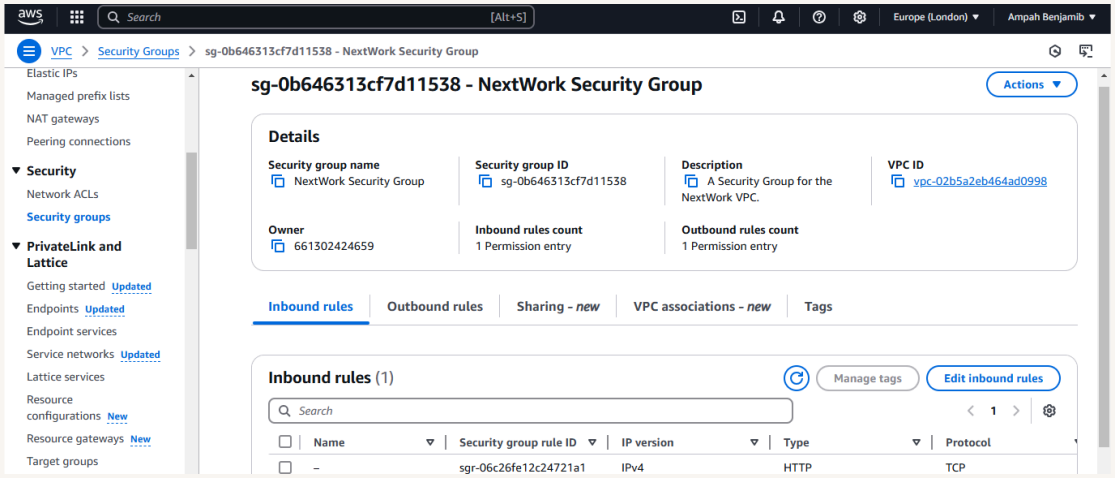
Security groups

Security groups are virtual firewalls that control inbound and outbound traffic for AWS resources. They define rules to allow or deny traffic based on IP, protocol, and port, ensuring secure communication within a VPC.

Inbound vs Outbound rules

Inbound rules are firewall rules that control incoming traffic to a resource based on IP, protocol, and port. I configured an inbound rule that allows HTTP (port 80) access from specific IPs for secure communication.

Outbound rules are firewall rules that control outgoing traffic from a resource based on IP, protocol, and port. By default, my security group's outbound rule allows all traffic (`0.0.0.0/0`), enabling unrestricted outbound communication.



Network ACLs

Network ACLs(Acces Control List) are stateless firewall rules that control inbound and outbound traffic at the subnet level in a VPC. They provide an additional layer of security by allowing or denying traffic based on rules evaluated in order.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are stateful and control traffic to a resource, while network ACLs are stateless and control traffic at the subnet level, evaluating rules in order for each request.

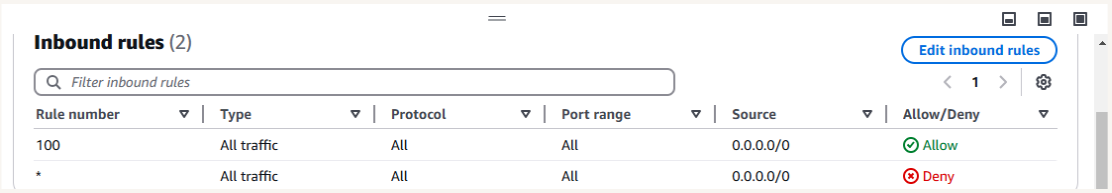
AM
ampahben3@gmail.com
NextWork Student

Default vs Custom Network ACLs

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

By default, a network ACL's(Acces Control List) inbound and outbound rules will allow all traffic (`0.0.0.0/0`) to flow in and out of the subnet until modified to restrict specific traffic.

In contrast, a custom ACL's (Acces Control List) inbound and outbound rules are automatically set to deny all traffic until specific rules are added to allow required communication.



Everyone should be in a job they love.

Check out nextwork.org for more projects