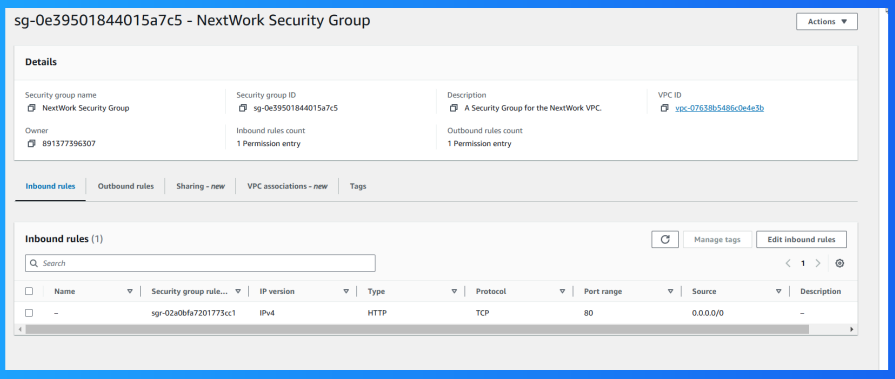
NextWork.org

VPC Traffic Flow and Security

Saish Nar



Saish Nar
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (VirtualPrivate Cloud) exists within an AWS region and is used to build a private and secure connection for resources in the subnets. Through an internet gateway, these resources and users can access internet to communicate each other.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to set up the flow of processes, which included creating a VPC, subnet, route table, internet gateway, security group, and network ACL.

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

One thing I did not expect in this project was, first, learning about different kinds of protocols and port numbers,and second, understanding the inbound and outbound rules for the custom network ACL.

This project took me...

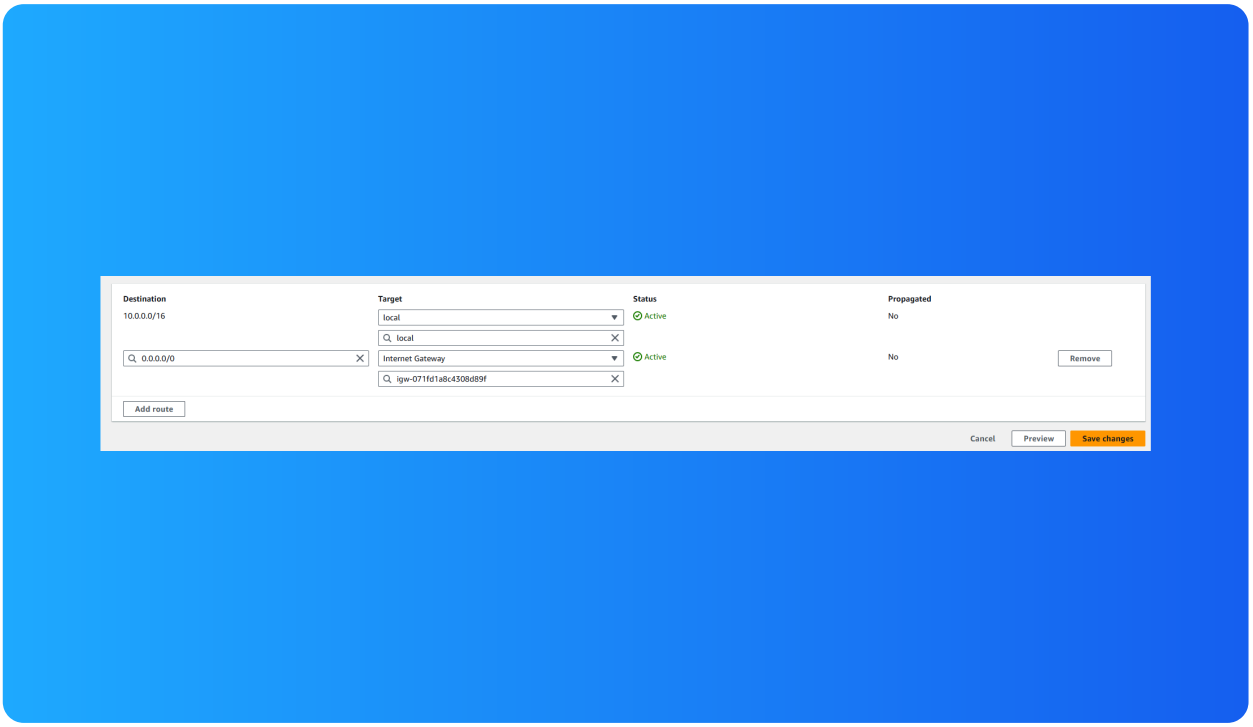
This project took me one and a half hour to complete.

Saish Nar
NextWork Student

Route tables

Route tables are like a GPS that directs traffic within my VPC to the correct destination.

Routes tables are needed to make a subnet public because a subnet needs to have a route to an internet gateway in order to be considered public. A route table is the only way to establish this connection.

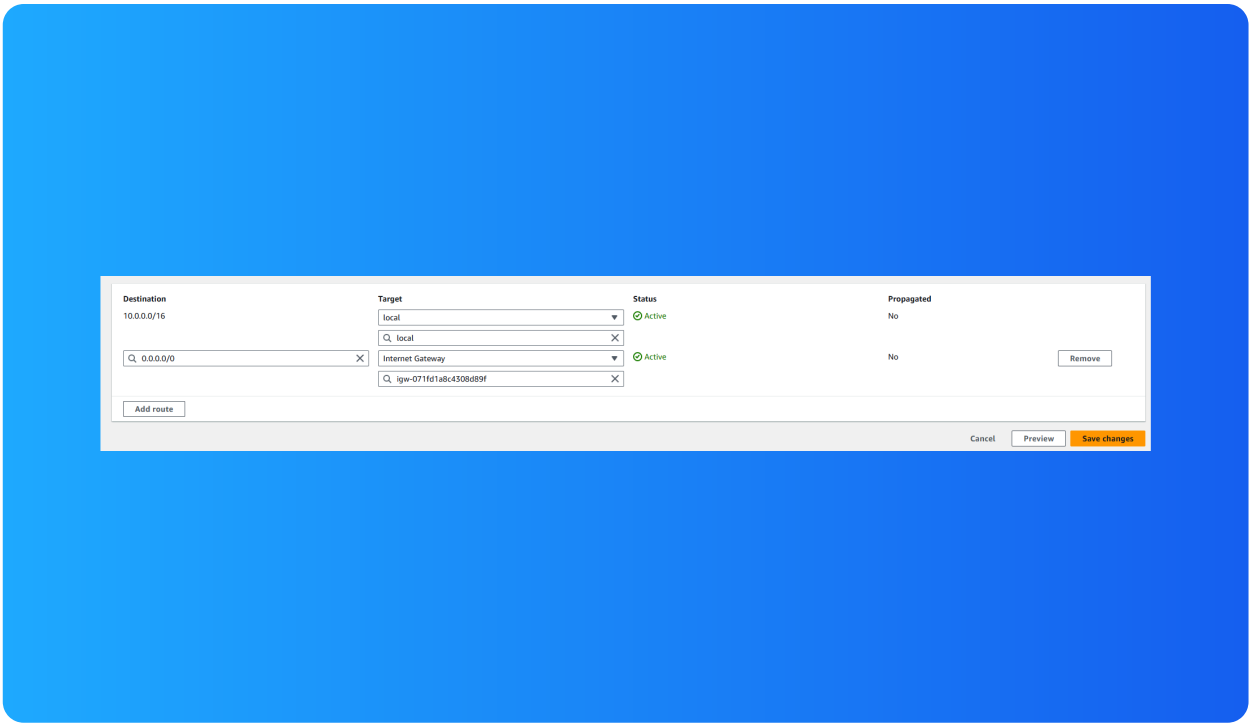


Saish Nar
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the destination is the range of IP addresses that traffic in my VPC is trying to reach. The target is the road or path that the traffic will use to get to their destination.

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 my NextWork IG (internet gateway).



Saish Nar
NextWork Student

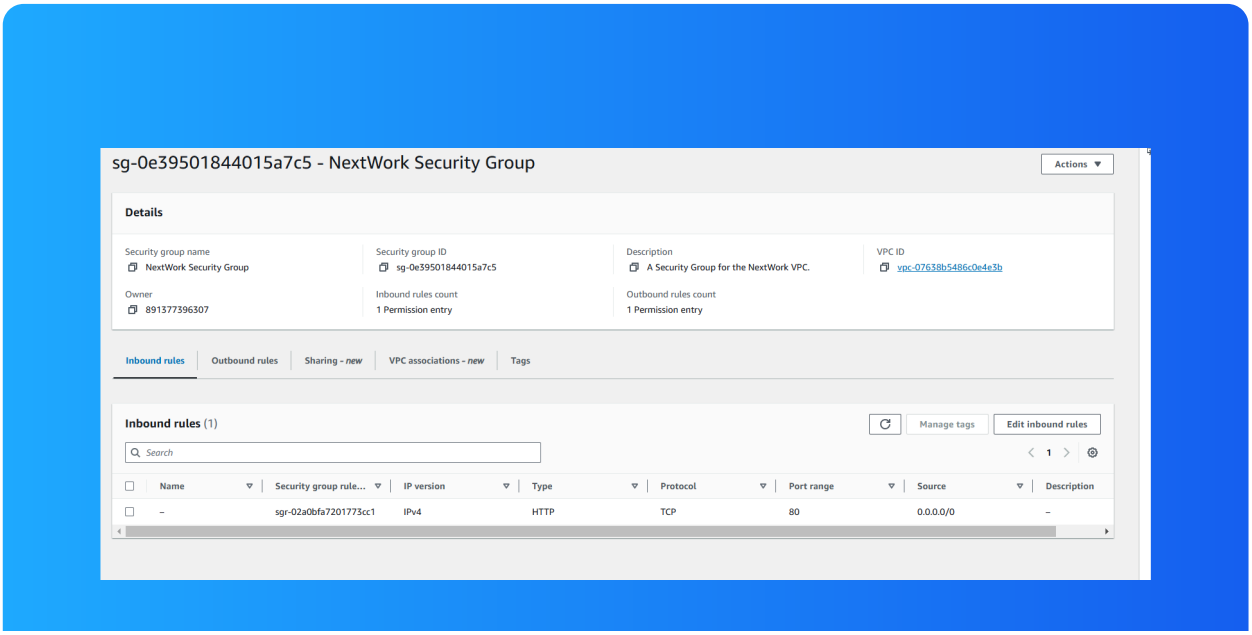
Security groups

Security groups are like security guards that monitor both inbound and outbound traffic at the resource level i.e. every single resource in a subnet or VPC has a security group.

Inbound vs Outbound rules

Inbound rules are the rules that monitor or restrict inbound traffic e.g. users visiting a web app I'm hosting. I configured an inbound rule that allows all inbound HTTP traffic.

Outbound rules are the rules that monitor or restrict outbound traffic e.g. my web app requesting data from a public source. By default, my security group's outbound rule allows all outbound traffic.



Saish Nar
NextWork Student

Network ACLs

Network ACLs are like community watchmen that secure my network at a subnet level.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that a security group secures my network at the resource level, which applies to all resources in a VPC, while a NACL secures my network at the subnet level, which applies to all subnets.

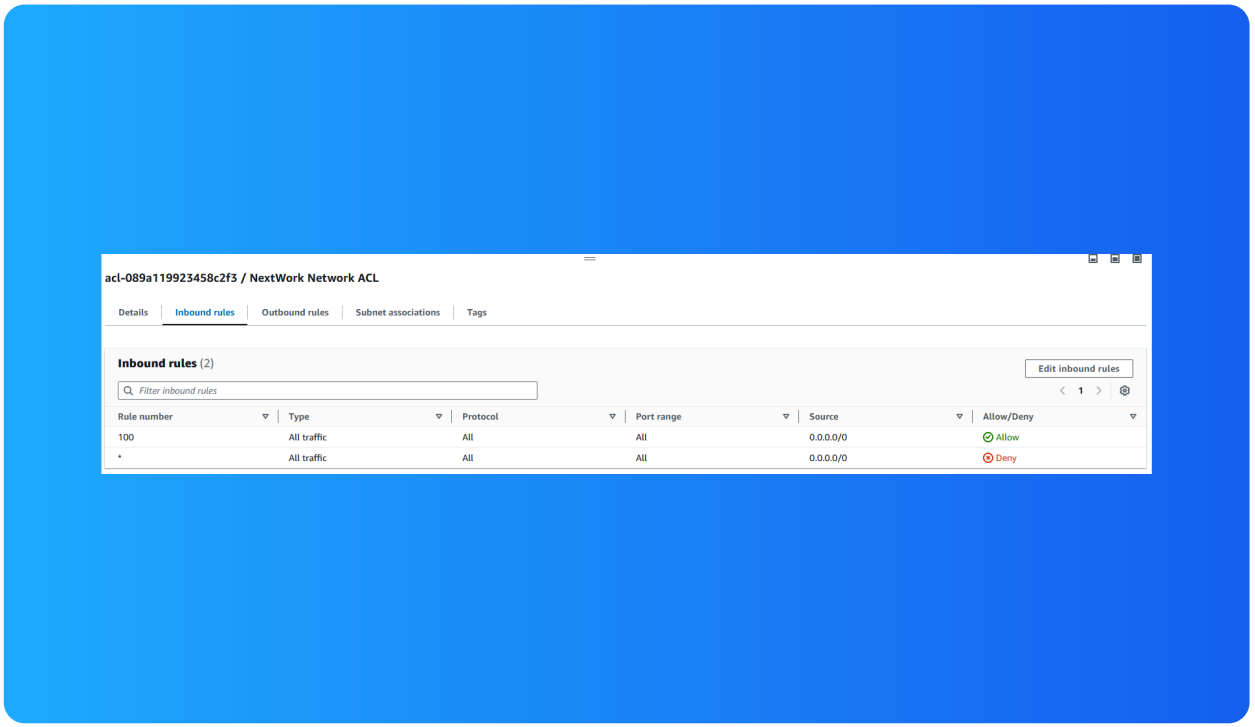
Saish Nar
NextWork Student

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 incoming and outgoing traffic.

In contrast, a custom ACL's inbound and outbound rules are set to deny all incoming and outgoing traffic by default.



Everyone should be in a job they love.

Check out nextwork.org for more projects