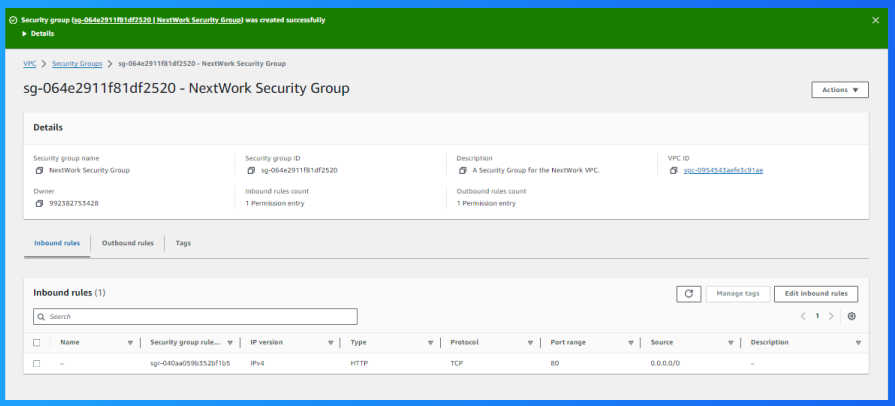
NextWork.org

VPC Traffic Flow and Security

Roshan Thomas



Roshan Thomas
NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is like your private internet castle in the cloud, where you control who gets in, what happens inside, and how data flows. It’s useful because it keeps your cloud resources secure and organized, just the way you want!

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to design a secure network. The "NextWork Security Group" manages traffic permissions, while the "NextWork route table" efficiently directs data within the VPC, ensuring a secure and organized network flow.

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

I didn't expect how seamlessly the VPC components, like route tables and network ACLs, would work together to manage traffic and secure the instance.

This project took me...

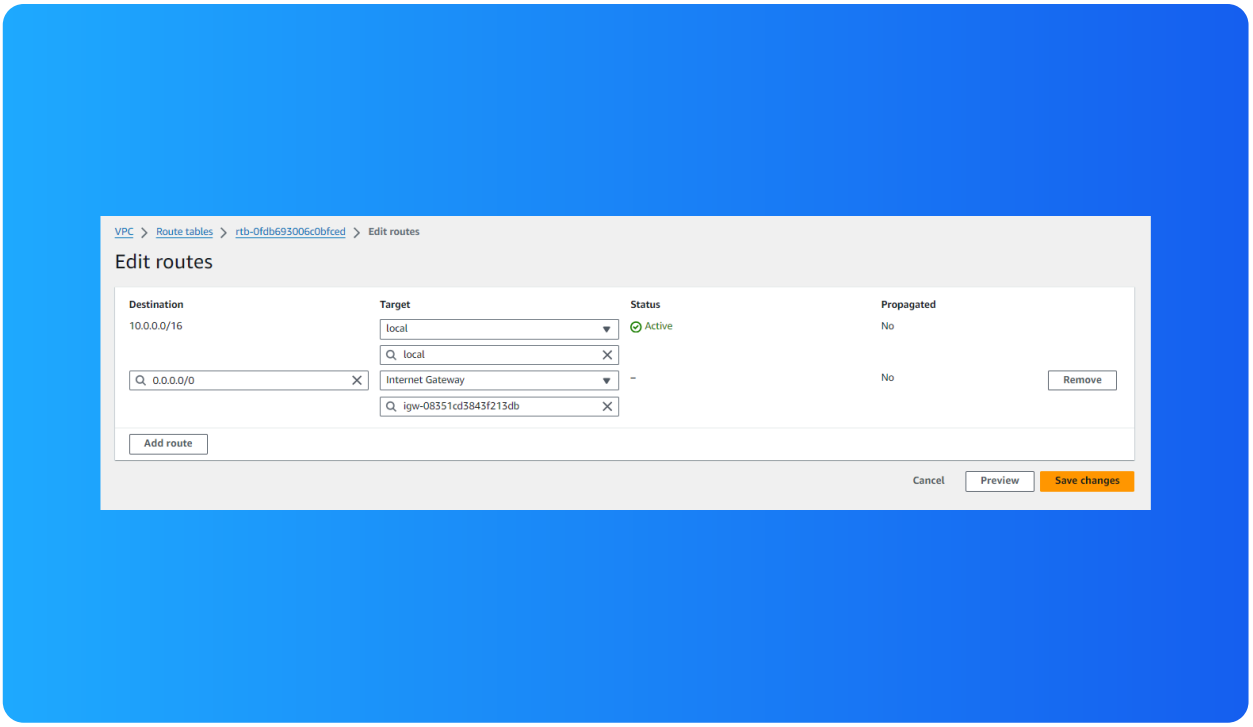
It took around 1 hour 45 minutes.

Roshan Thomas
NextWork Student

Route tables

Route tables are the maps that guide traffic in my VPC, telling data where to go. They ensure everything finds its way, like a GPS system for my virtual city's network!

Route tables are needed to make a subnet public because they create the path to the internet. Without them, my subnet's traffic would be stuck in the neighborhood, unable to reach the outside world!



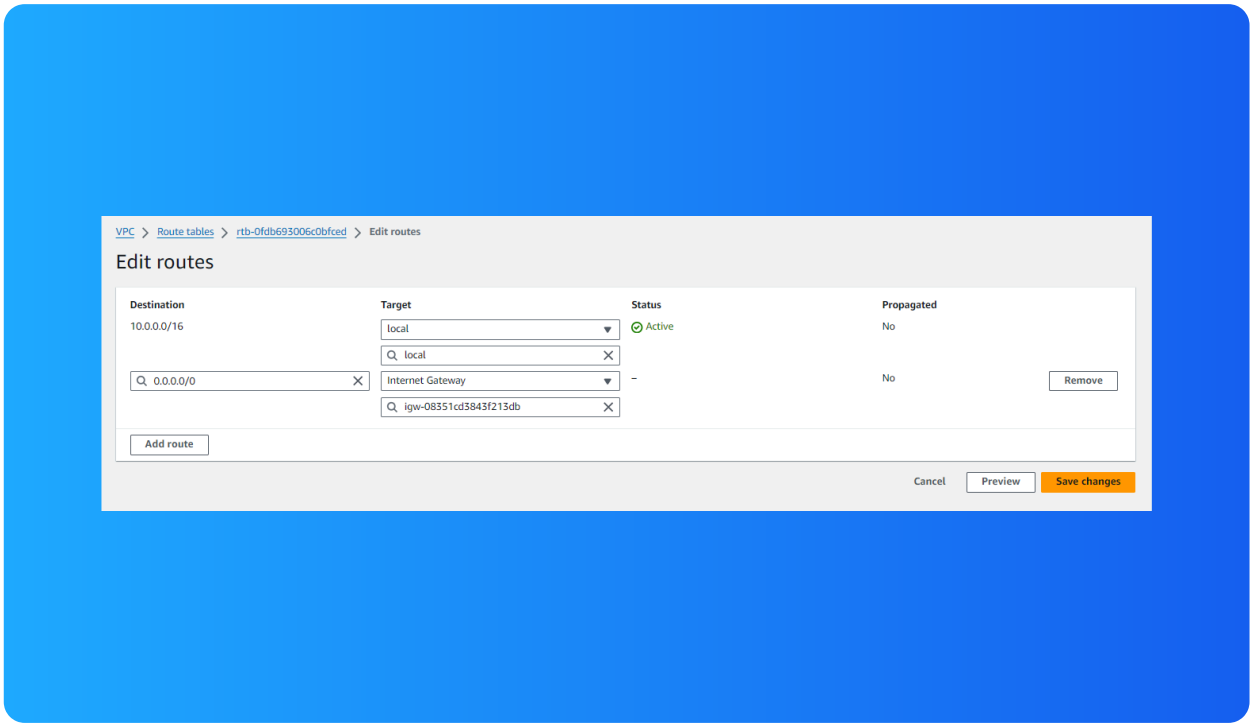
Roshan Thomas
NextWork Student

NextWork.org

Route destination and target

Routes are defined by their destination and target, which mean the final address where the traffic is headed and the path it should take to get there. It's like setting a trip's endpoint and choosing the road to drive on!

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 Internet Gateway.



Roshan Thomas
NextWork Student

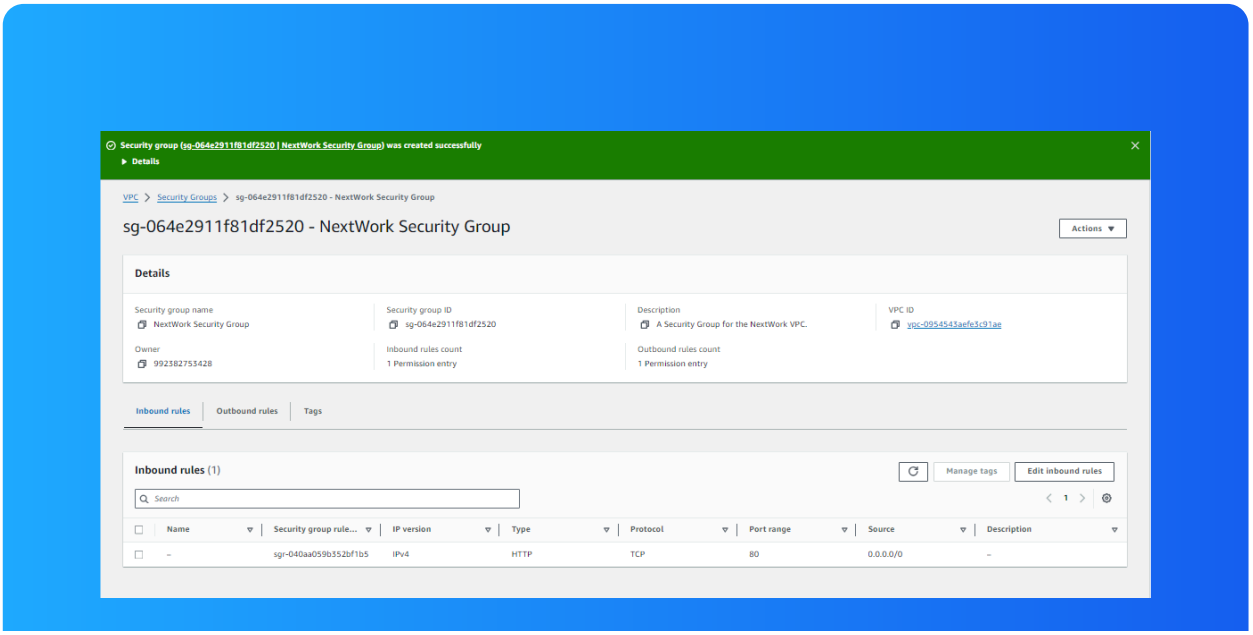
Security groups

Security groups are the bodyguards of my AWS resources, controlling who gets in and out. They act as virtual bouncers, enforcing the rules to keep my cloud environment safe and sound!

Inbound vs Outbound rules

Inbound rules are the permissions that control what traffic can enter my resources. I configured an inbound rule that allows anyone on the internet in, like a bouncer letting in all the party guests without checking the guest list!

Outbound rules are the permissions that control what traffic can leave my resources. By default, my security group's outbound rule allows all traffic out, like an open gate letting everything exit freely!



Roshan Thomas
NextWork Student

NextWork.org

Network ACLs

Network ACLs are the security fences around my VPC, controlling traffic at the subnet level. They're like neighborhood watch guards, checking who's allowed to pass through and who's not!

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are like personal bodyguards for each resource, while network ACLs are the neighborhood watch, overseeing entire subnets and enforcing broader rules!

Roshan Thomas
NextWork Student

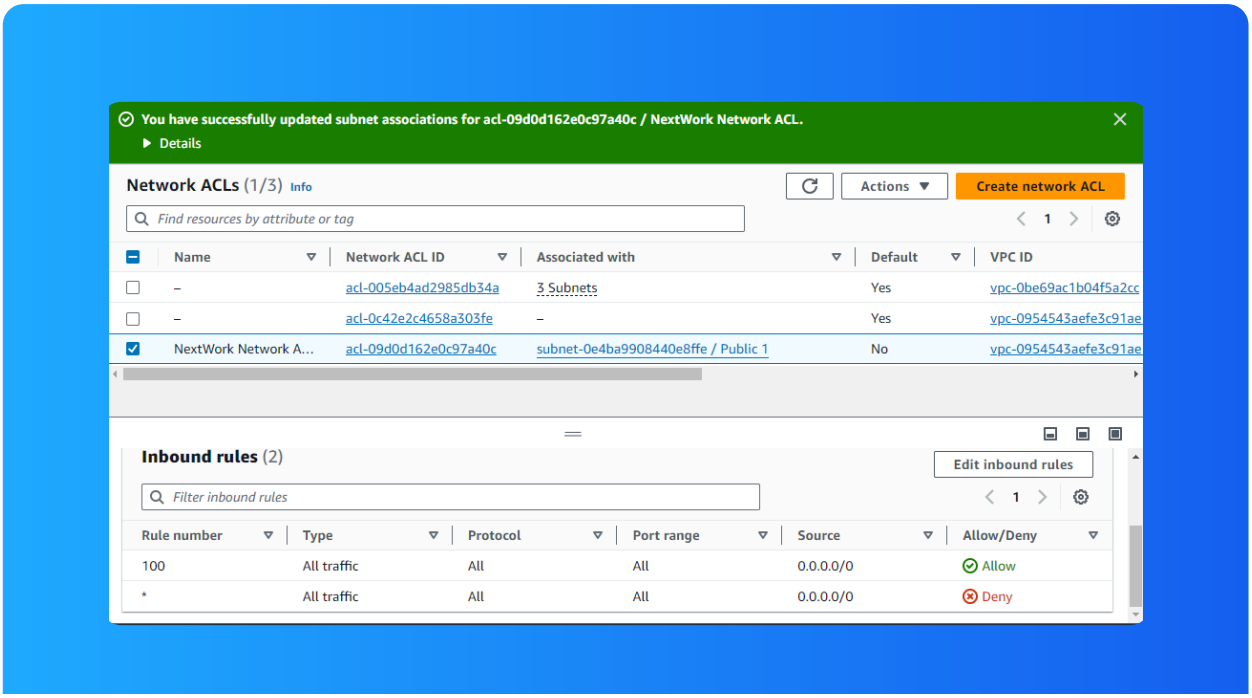
NextWork.org

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 flow freely, like an open gate with no restrictions, letting everything in and out without any checks!

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic, both in and out. You have to manually configure the rules to allow or deny specific traffic. It's like being the gatekeeper, deciding who gets in or out



Everyone should be in a job they love.

Check out nextwork.org for more projects