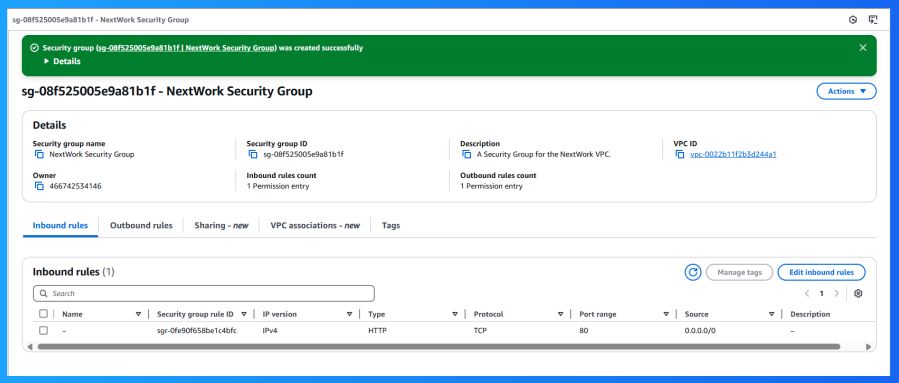
NextWork.org

VPC Traffic Flow and Security

DI dineshrajdhanapathy@gmail.com



DI
dineshrajdhanapathy@g...
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a service that lets you create a private network in AWS, enabling secure, isolated environments for your resources. It's useful for controlling traffic, security, and network design.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private network. I set up subnets, route tables, and an internet gateway for internet access. I configured security groups and network ACLs for traffic control and security.

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

One thing I didn't expect in this project was the level of detail required to configure security groups and network ACLs properly. Ensuring the right balance between accessibility and security was more complex than anticipated.

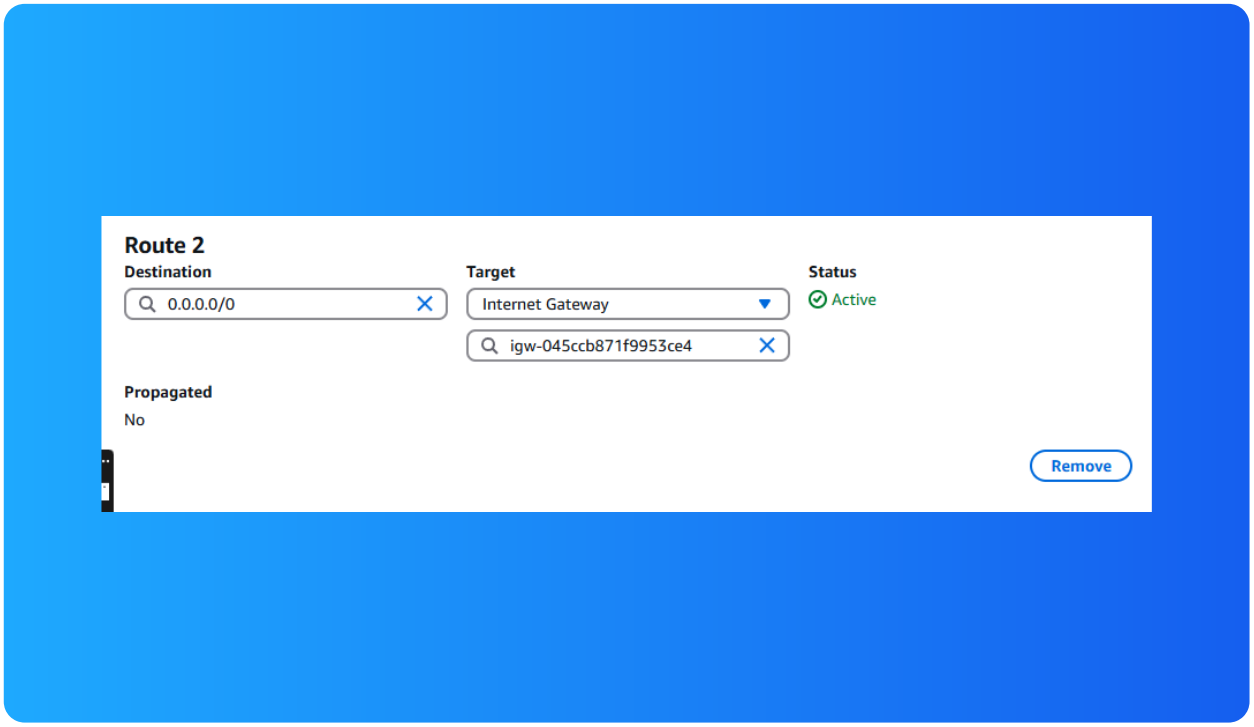
This project took me...

This project took me about 1-2 hours. It involved setting up the VPC, configuring subnets, route tables, security groups, and network ACLs, as well as testing connectivity and troubleshooting any issues along the way.

Route tables

Route tables are essential components in networking that determine how data packets are directed within a network. They consist of rules,called routes,specifying paths for traffic to reach its destination,ensuring communication between devices & nw.

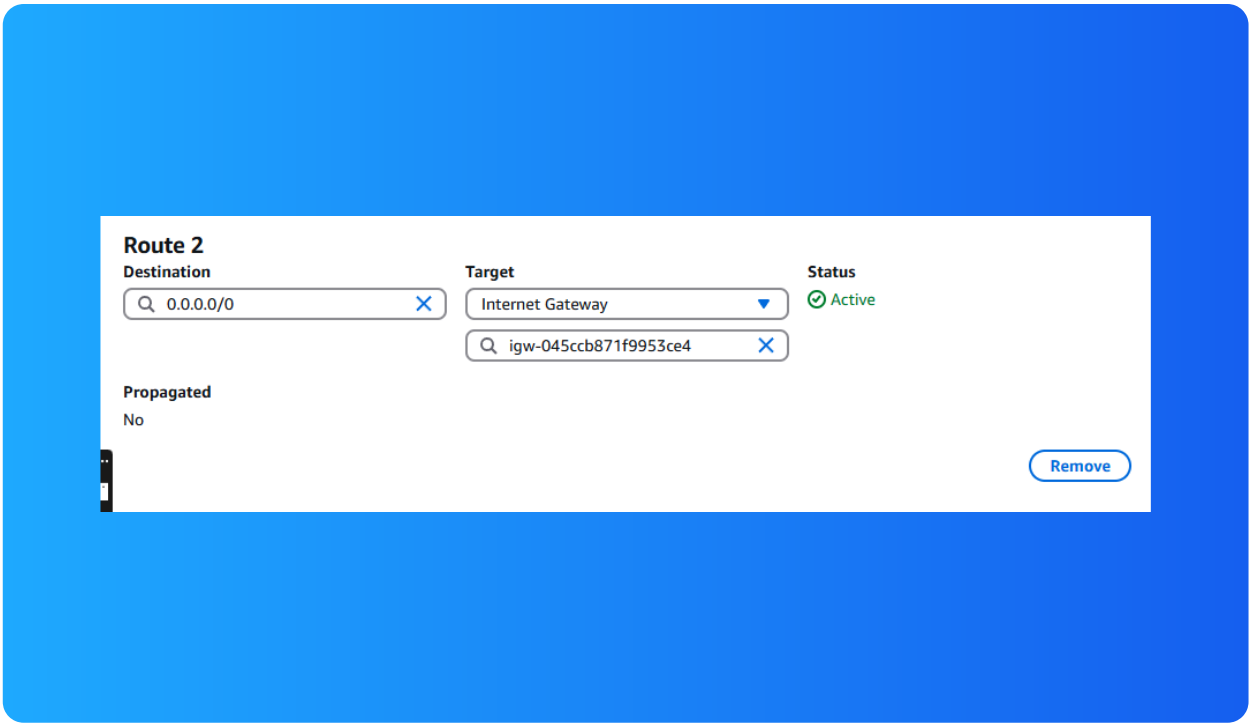
Route tables are needed to make a subnet public because they define a route directing internet-bound traffic to an internet gateway, enabling external connectivity for resources in the subnet.



Route destination and target

Routes are defined by their destination and target, which mean the IP range or address to reach (destination) and the next-hop resource (target) like an internet gateway or virtual appliance that forwards the traffic.

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 (e.g., igw-xxxxxxxx).



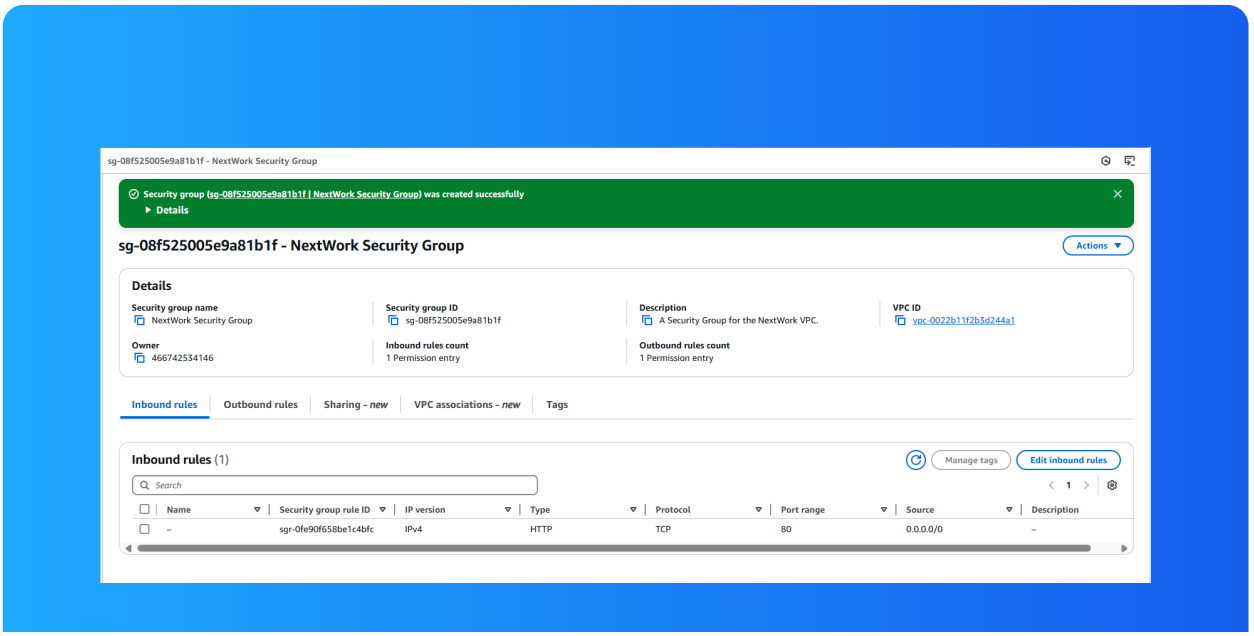
Security groups

Security groups are virtual firewalls that control inbound and outbound traffic for resources in a network, allowing or denying traffic based on specified rules for enhanced security.

Inbound vs Outbound rules

Inbound rules are permissions that specify the traffic allowed to enter a resource. I configured an inbound rule that permits HTTP traffic on port 80 from any source (0.0.0.0/0).

Outbound rules are permissions that specify the traffic allowed to leave a resource. By default, my security group's outbound rule allows all traffic to any destination (0.0.0.0/0).



Network ACLs

Network ACLs are optional subnet-level firewalls in a VPC that control inbound and outbound traffic with stateless rules applied to all resources in the subnet.

Security groups vs. network ACLs

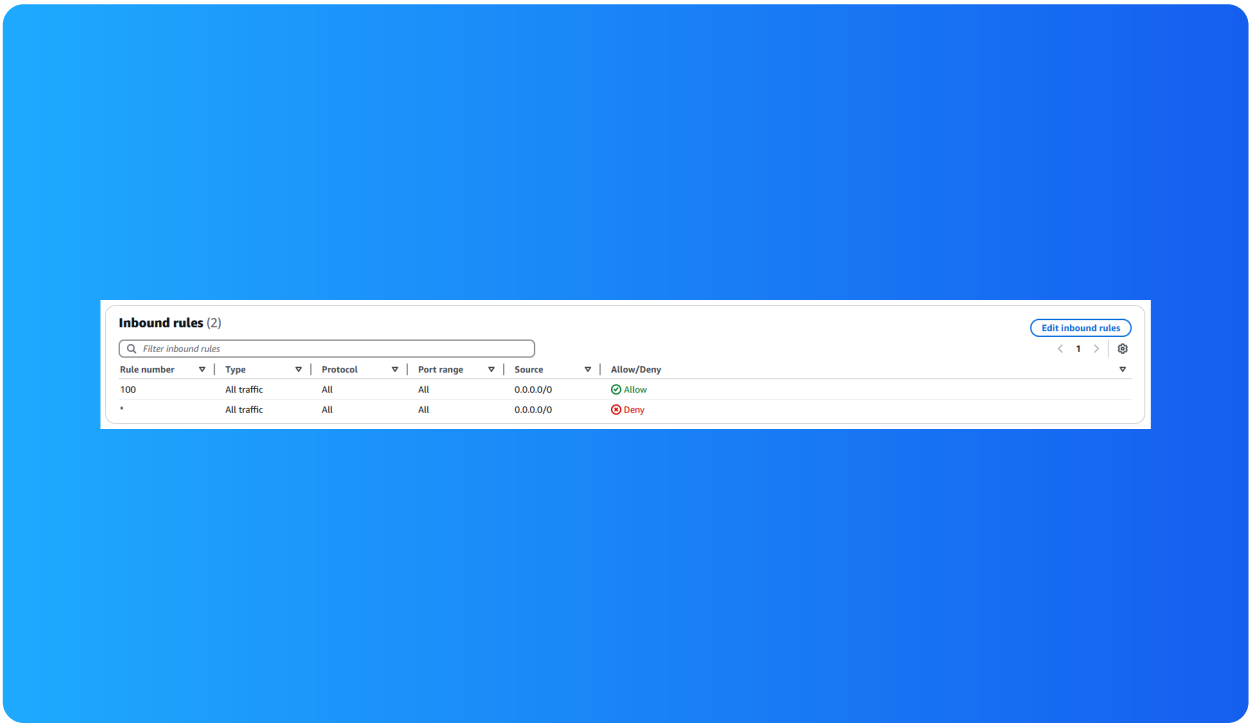
The difference between a security group and a network ACL is that security groups are stateful and applied to individual resources, while network ACLs are stateless and operate at the subnet level, affecting all resources within it.

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 and from any source (0.0.0.0/0).

In contrast, a custom ACL’s inbound and outbound rules are automatically set to deny all traffic. must explicitly configure the rules to allow traffic, specifying IP ranges, protocols & port numbers for inbound & outbound connections to destinations.



Everyone should be in a job they love.

Check out nextwork.org for more projects