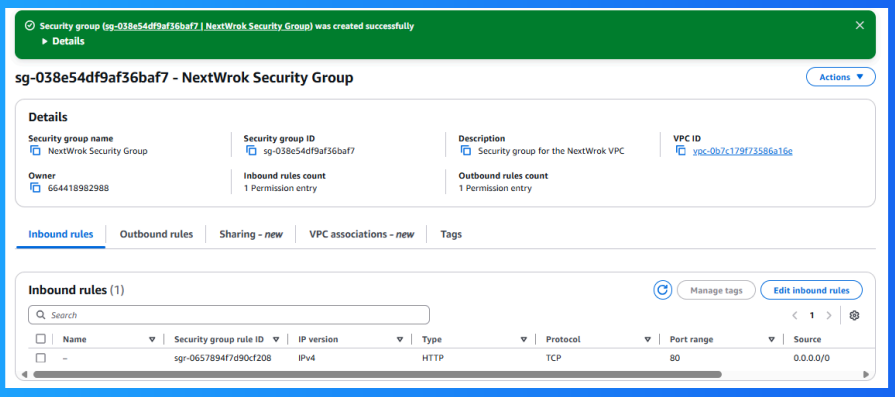
NextWork.org

VPC Traffic Flow and Security

IT itsbryantgonzalez@gmail.com



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is useful because this creates a layer of security and privacy for your assets. This is the equivalent of creating a gated community for your assets.

How I used Amazon VPC in this project

I used Amazon VPC to create security groups and ACLS for the inbound and outbound traffic communicating with my VPC.

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

One thing I didn't expect in this project was how easy to use AWS is.

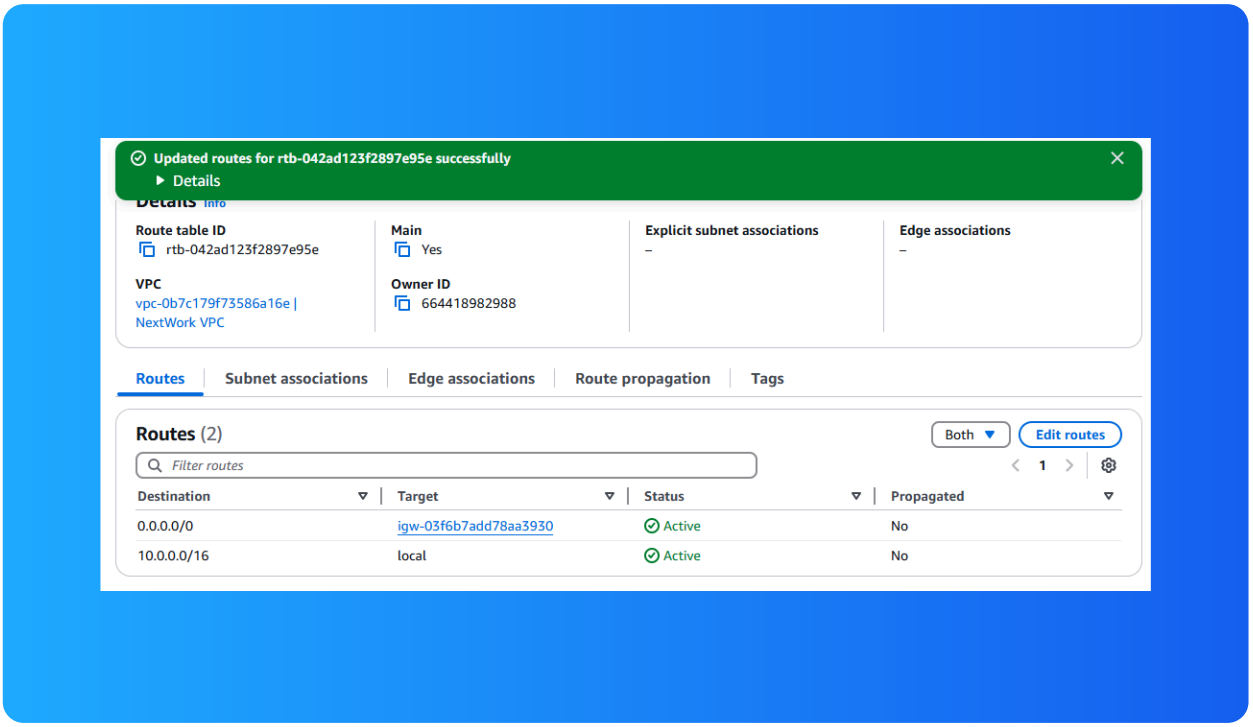
This project took me...

This project took a little more than an hour to complete.

Route tables

Route tables are equivalent to highways or a GPS system. Essentially they make it easier for IP addresses to efficiently communicate with the internet gateway.

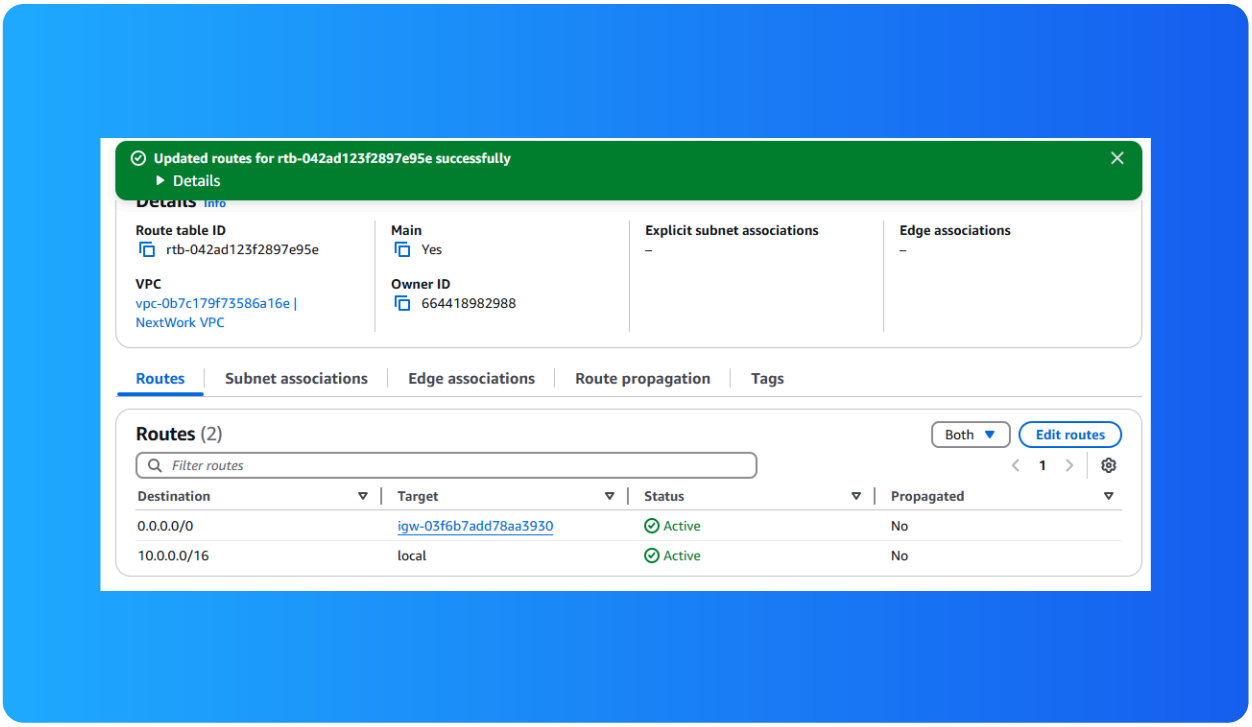
Route tables are needed to make a subnet public because a subnet needs to have a route to an internet gateway to be considered public. A routing table is the only way to establish this connection.



Route destination and target

Routes are defined by their destination and target which means the destination is the range of IP ranges that you want to route and the target is the path they will take which is the internet gateway.

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of Ip ranges which is 0.0.0.0/0 and a target of NextWork IG (Internet gateway).



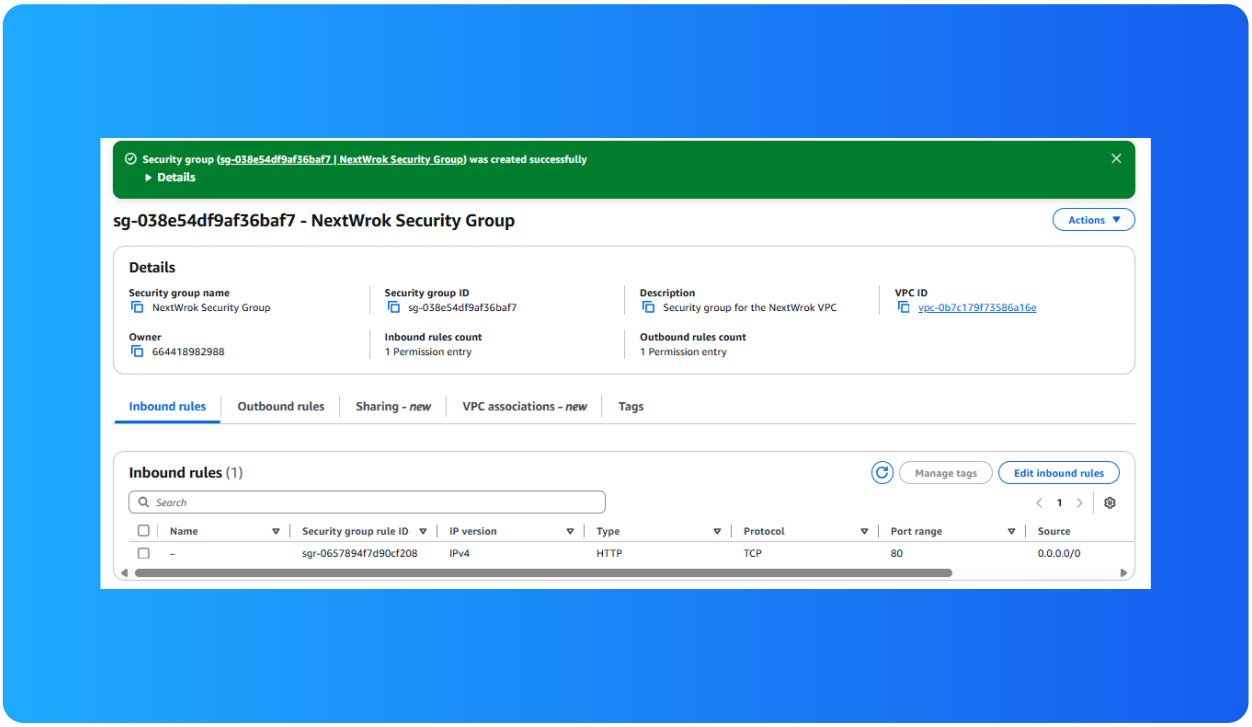
Security groups

Security groups are rule sets for assigned sections of traffic. This can be for inbound or outbound traffic.

Inbound vs Outbound rules

Inbound rules are to restrict or allow certain types of traffic. I configured an inbound rule over port 80 (HTTP) that allows for inbound traffic to communicate with our VPC.

Outbound rules rules to restrict or allow outgoing traffic outside the VPC. By default my security group's outrule allows all traffic.



Network ACLs

Network ACLS are a set of rules to restrict or allow inbound/outbound traffic for the VPC.

Security groups vs. network ACLs

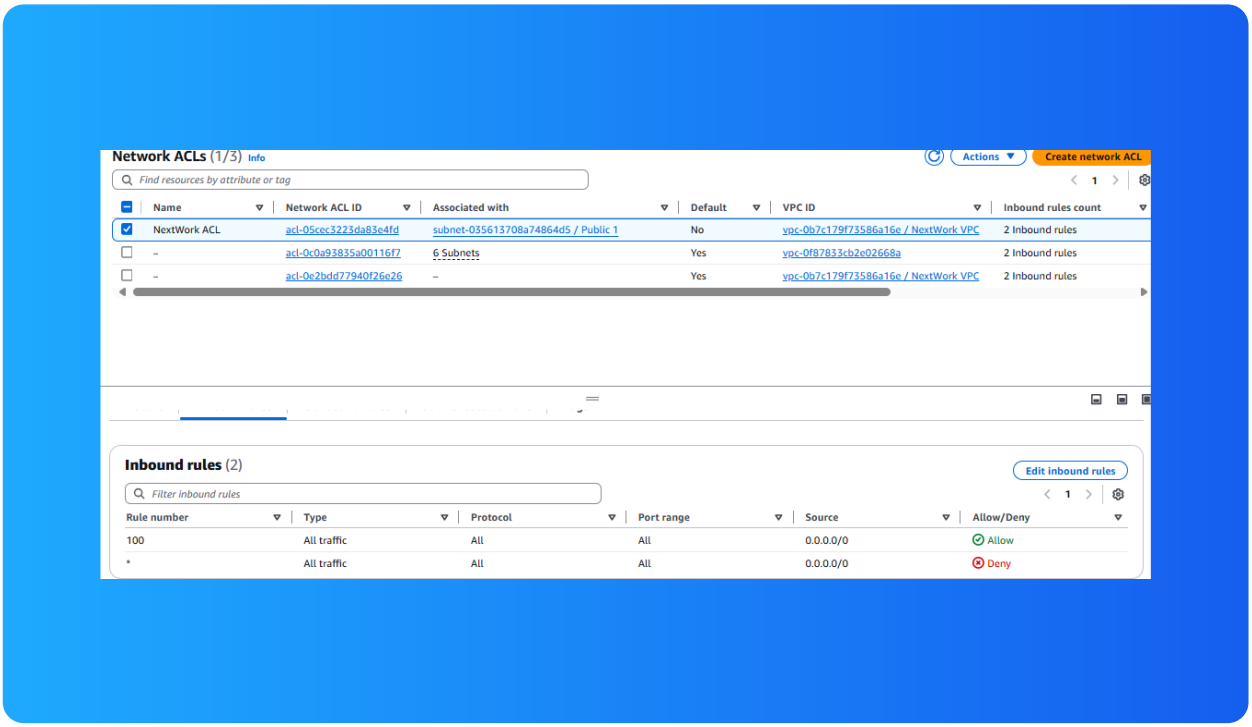
The difference between a security group and a Network ACL is that they secure networks at different levels. Network ACL secure subnet layer traffic and security groups secure traffic accessing traffic accessing assets in the VPC.

Default vs Custom Network ACLs

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

By default a network ACLS's inbound and outbound rules will deny inbounc and outbound traffic until you add a rule to allow the traffic in and out of your VPC.

In contast, a custom ACL's inbound and outbound rules are automatically set to allow.



Everyone should be in a job they love.

Check out nextwork.org for more projects