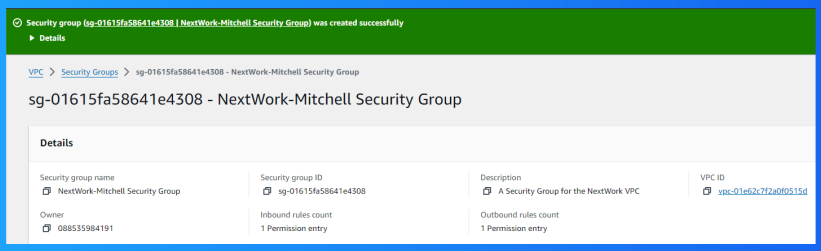
NextWork.org

VPC Traffic Flow and Security

mmoorejr24@gmail.com



Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud (AWS VPC) gives you full control over your virtual networking environment, including resource placement, connectivity, and security.

How I used Amazon VPC in this project

I used it AWS VPC to setup a public subnet to connect to the internet. I had to configure a routing table to connect to the internet gateway so that it would connect to the internet. Also setup security groups and ACL for traffic security.

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

I didn't expect this project to be so massive and complex. Looks like a lot of things happen under the hood that needs to be configured.

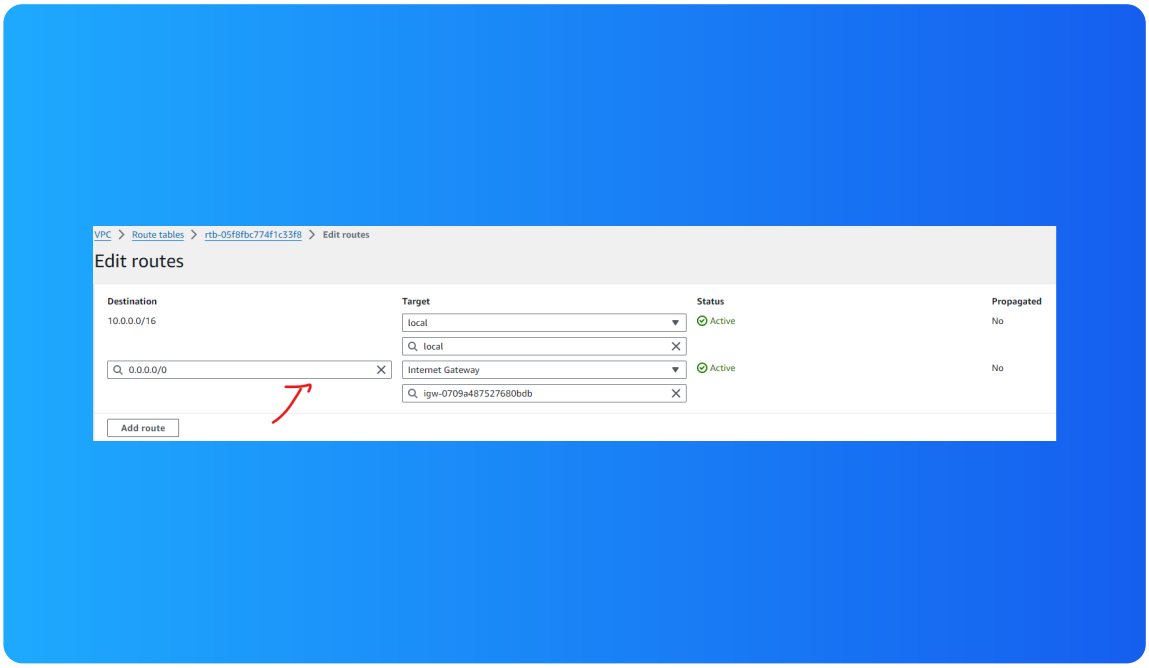
This project took me...

This project took about 1 hour and 45 mins to complete.

Route tables

Route tables are tables of rules, called routes, that decide where the data in your network should go.

Routes tables are needed to make a subnet public because now it knows how to access the internet gateway to be accessed by the internet.

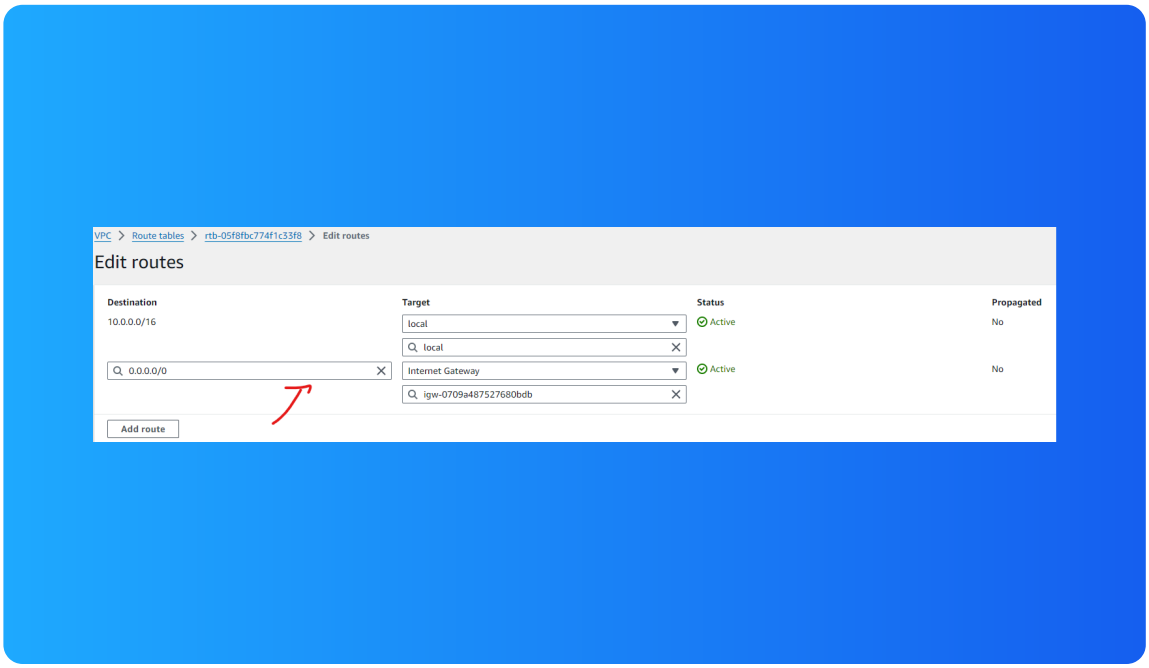


mmoorejr24@gmail.com
NextWork Student
NextWork.org

Route destination and target

Routes are defined by their destination and target, which mean that control where the traffic is going from subnet to internet.

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 igw-0709a487527680bdb.



mmoorejr24@gmail.com
NextWork Student

NextWork.org

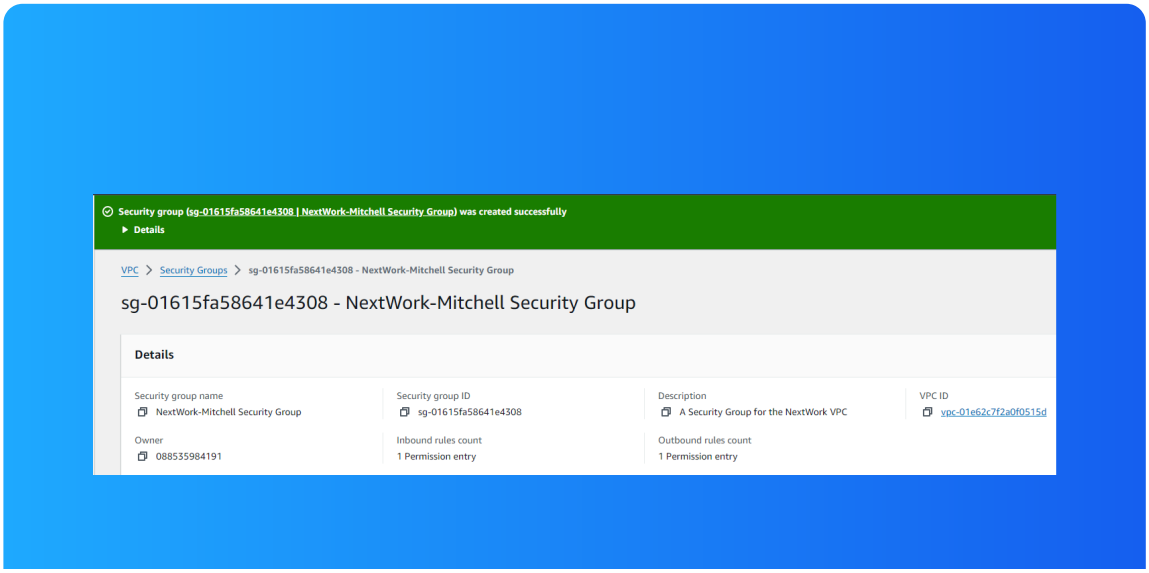
Security groups

Security groups are responsible for monitoring both inbound traffic and outbound traffic at the resource level i.e every single resource in a subnet/VPC has a security group.

Inbound vs Outbound rules

Inbound rules are the rules that monitor/restrict inbound traffic e.g users visiting a web app I am hosting. I configured an inbound rule that allows all IP addresses to access the subnet.

Outbound rules are the rules that monitor/restrict outbound traffic. By default, my security group's outbound rule will allow all outbound traffic.



mmoorejr24@gmail.com
NextWork Student
NextWork.org

Network ACLs

Network ACLs are used to set broad traffic rules that apply to an entire subnet, checking each data packet against a table of ACL rules before allowing them through

Security groups vs. network ACLs

The difference between a security group and a network ACL is that it sets broad traffic rules that apply to an entire subnet. Security groups allow for more granular control, managing access to individual resource.

mmoorejr24@gmail.com
NextWork Student

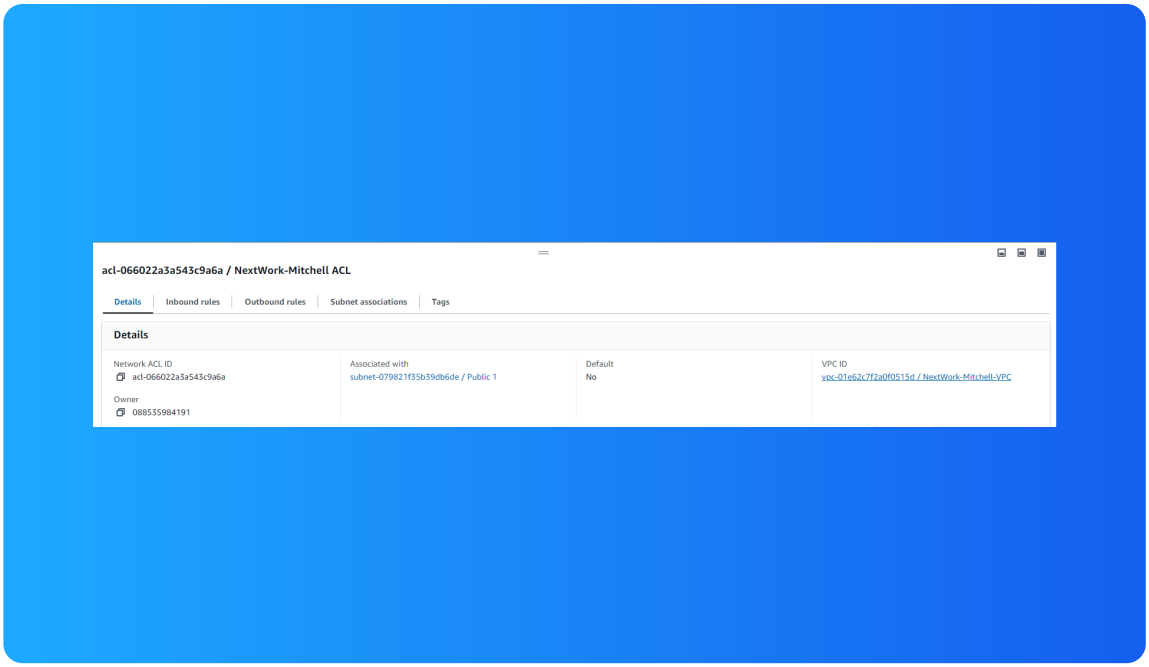
NextWork.org

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 incoming and outgoing traffic.

In contrast, a custom ACLâ▤▤s inbound and outbound rules are automatically set to deny all incoming and outgoing traffic.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects