NextWork.org

VPC Traffic Flow and Security

PH phogan2886@gmail.com

PH

phogan2886@gmail.com
NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

VPC is a service that allows users to create a virtual network in the AWS cloud that's isolated from other virtual networks. Users can then launch AWS resources, such as EC2 and Database Service (RDS) instances into this virtual network

How I used Amazon VPC in this project

I created Access Control List and set inbound and outbound rules for the subnets associated with them

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

The ease on how to set up the rules for the subnets we had created

This project took me...

took me about 30 minutes to complete

PH

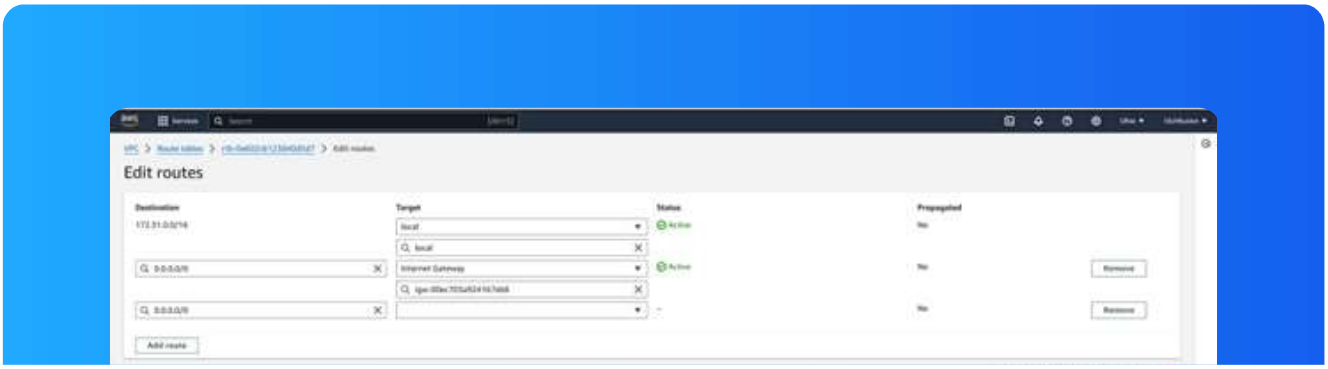
phogan2886@gmail.com
NextWork Student

NextWork.org

Route tables

Route tables are a set of routes that determine how traffic is routed from one point to another in a network

route tables are used to make a subnet public by sending all traffic to the internet gateway. A route table is a set of rules that determine where network traffic is directed. Each route in a route table specifies the destination and the target.



PH

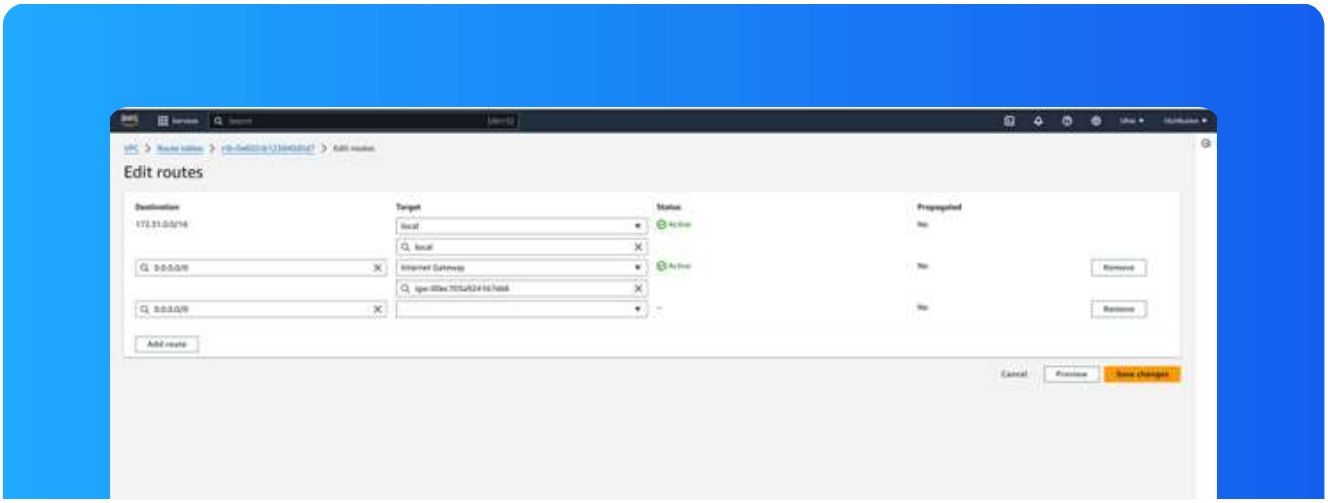
phogan2886@gmail.com
NextWork Student

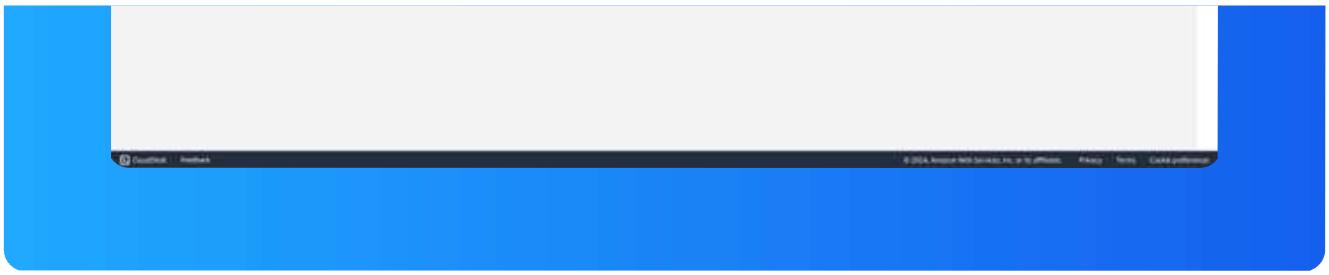
NextWork.org

Route destination and target

Routes are defined by their destination and target, which mean The target can be the connection through which the traffic will cross. The destination is the IP address or range of IP addresses to which the network traffic can be redirected.

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of default internet gateway and a target of the subnet





PH

phogan2886@gmail.com
NextWork Student

NextWork.org

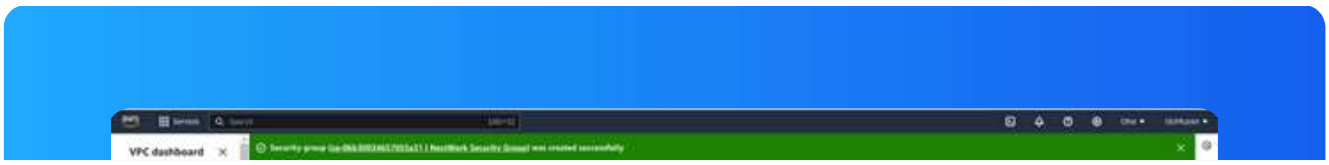
Security groups

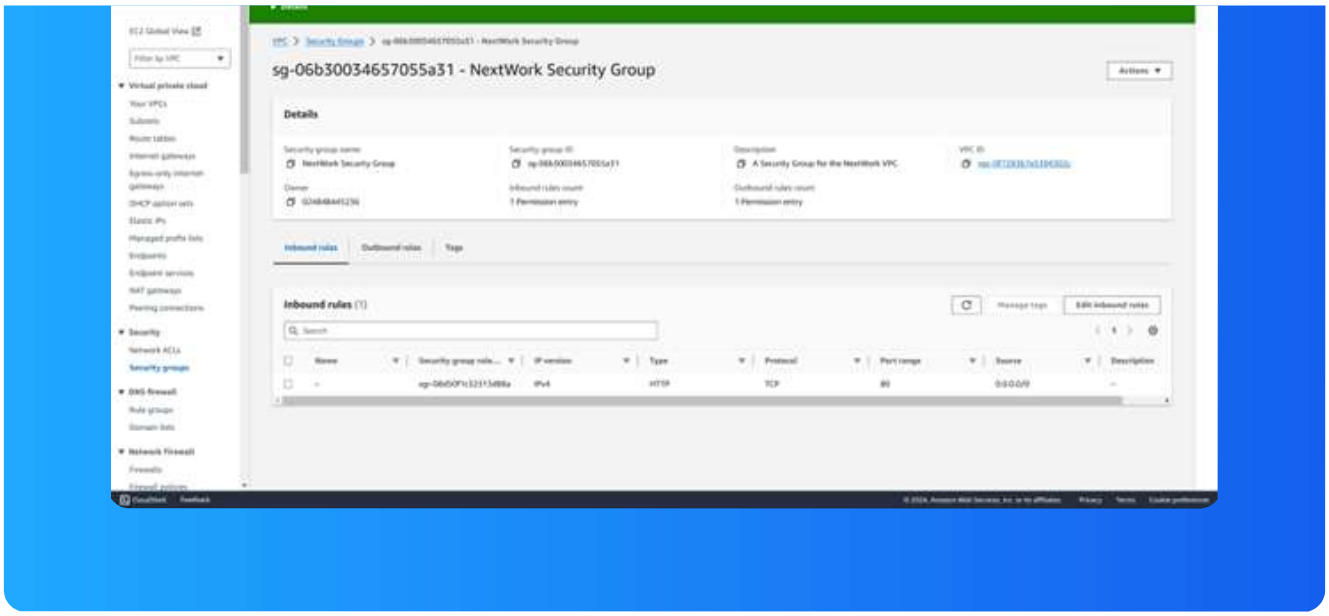
Security groups are a security checkpoint, or security guard, at the entrance for each building (resource) in that neighbourhood (subnet).

Inbound vs Outbound rules

Inbound rules control the data that can enter the resources in your security group. I configured an inbound rule that setting the source to "0.0.0.0/0", allows any IP address to access your resource.

Outbound rules control that data that your resources can send out. By default, my security group's outbound rule allow all outbound traffic





PH

phogan2886@gmail.com
NextWork Student

NextWork.org

Network ACLs

Network ACLs are a set of rules that control access to a network, similar to a guest list at a club.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups control traffic at the instance level, while ACLs control traffic at the VPC subnet level.

PH

phogan2886@gmail.com
NextWork Student

NextWork.org

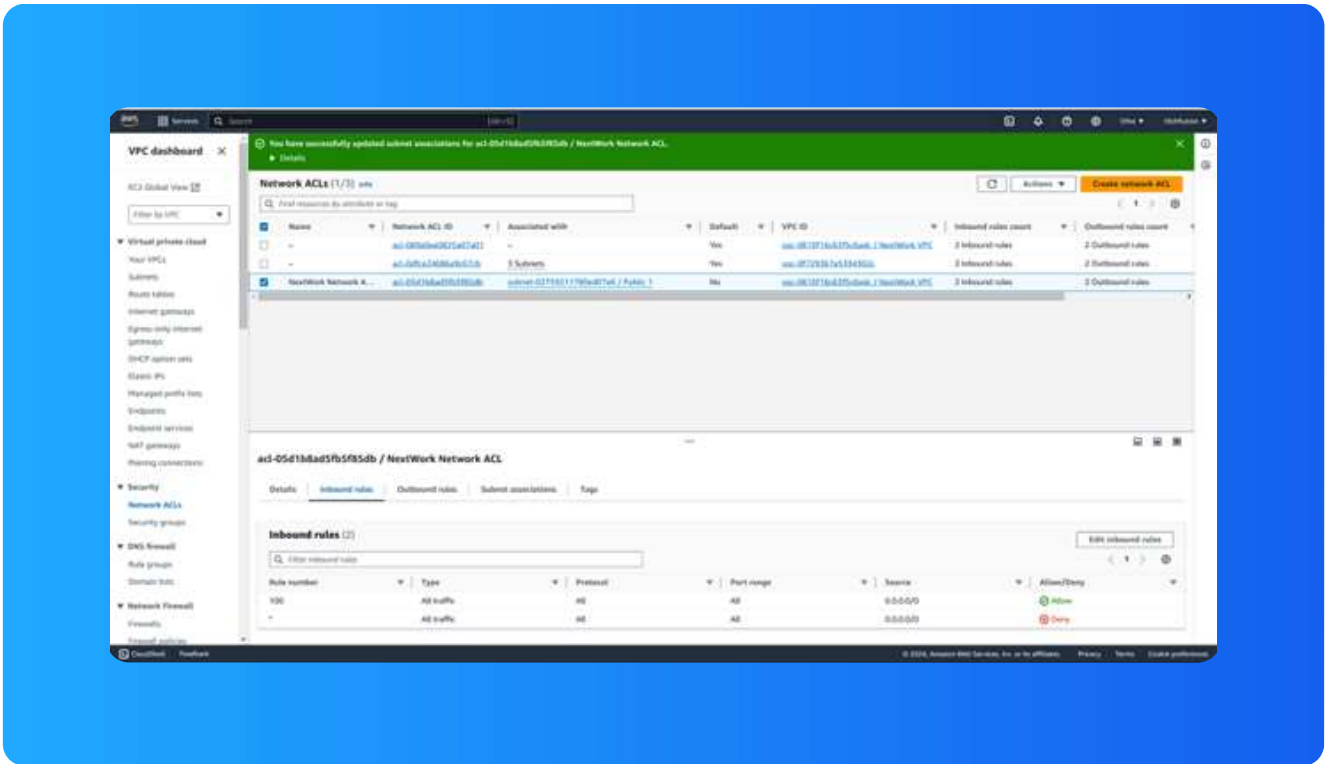
Default vs Custom Network ACLs

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

The default network access control list for VPC allows all inbound and outbound traffic to flow in and out of associated subnets. The default ACL also includes a rule with an asterisk that denies packets that don't match any other rules

A custom network access control list in VPC denies all inbound and outbound traffic by default, unless rules are configured. Once rules are created and the

ACL is associated with a subnet, the rules evaluate any inbound or outbound traffic



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects