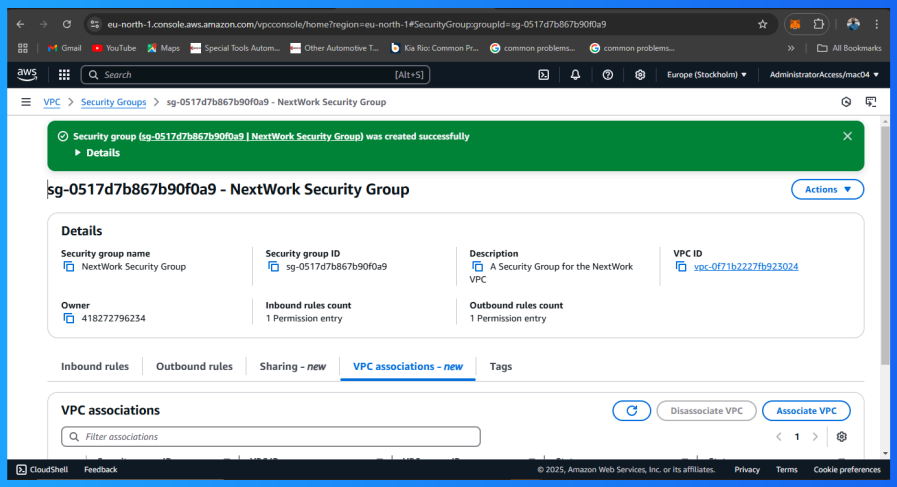
NextWork.org

VPC Traffic Flow and Security

Michael Emeruwa



Michael Emeruwa
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private network in the cloud. It provides a means to control traffic interaction with data on the network.

How I used Amazon VPC in this project

I created my own Amazon VPC and set up traffic flow and security.

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

I didn't expect the inbound and outbound rules to decline all traffic by default.

This project took me...

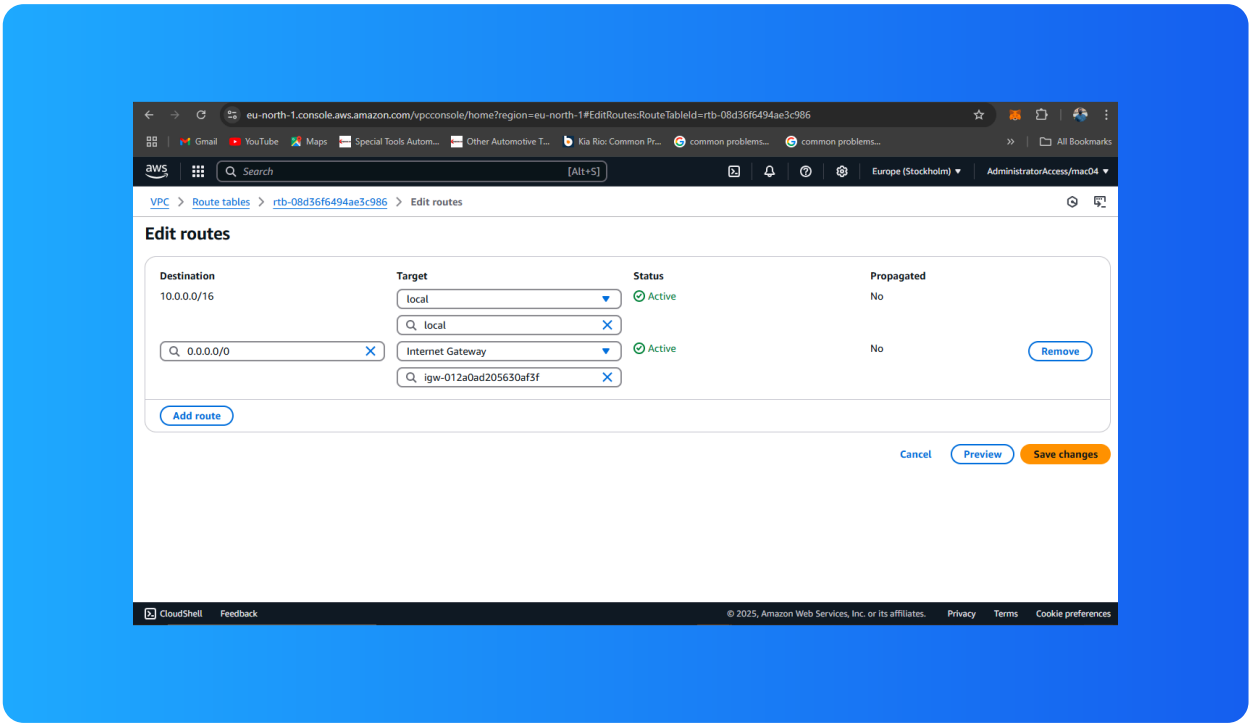
40mins

Michael Emeruwa
NextWork Student

Route tables

Route tables are path ways for resources within the network to share and receive data.

Routes tables are needed to make a subnet public because without it, there's no pathway for incoming traffic. External users would not be able to accesss the data.

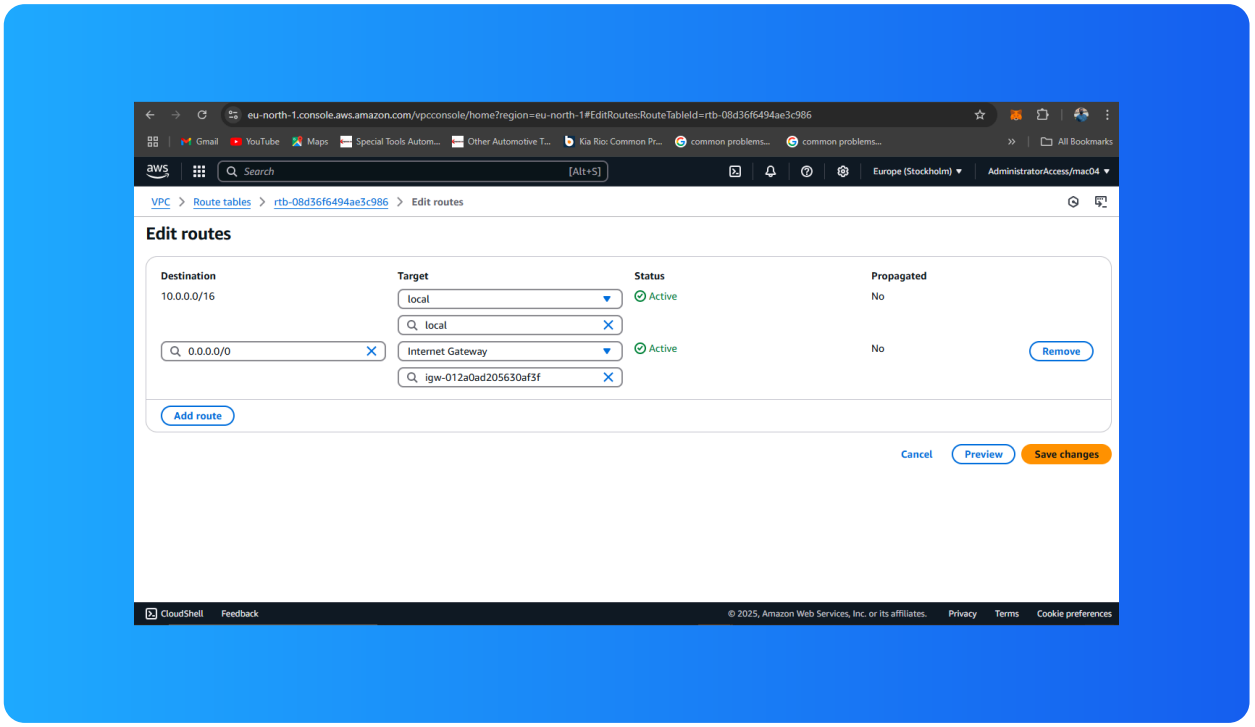


Michael Emeruwa
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the IP address range for traffic and the path traffic has to take to get there. The target can either route traffic to the internet or keep traffic within the VPC.

The route in my route table that directed internet-bound traffic to my internet gateway had a estination of 0.0.0.0/0 and a target of igw-012a0ad20563af3f



Michael Emeruwa
NextWork Student

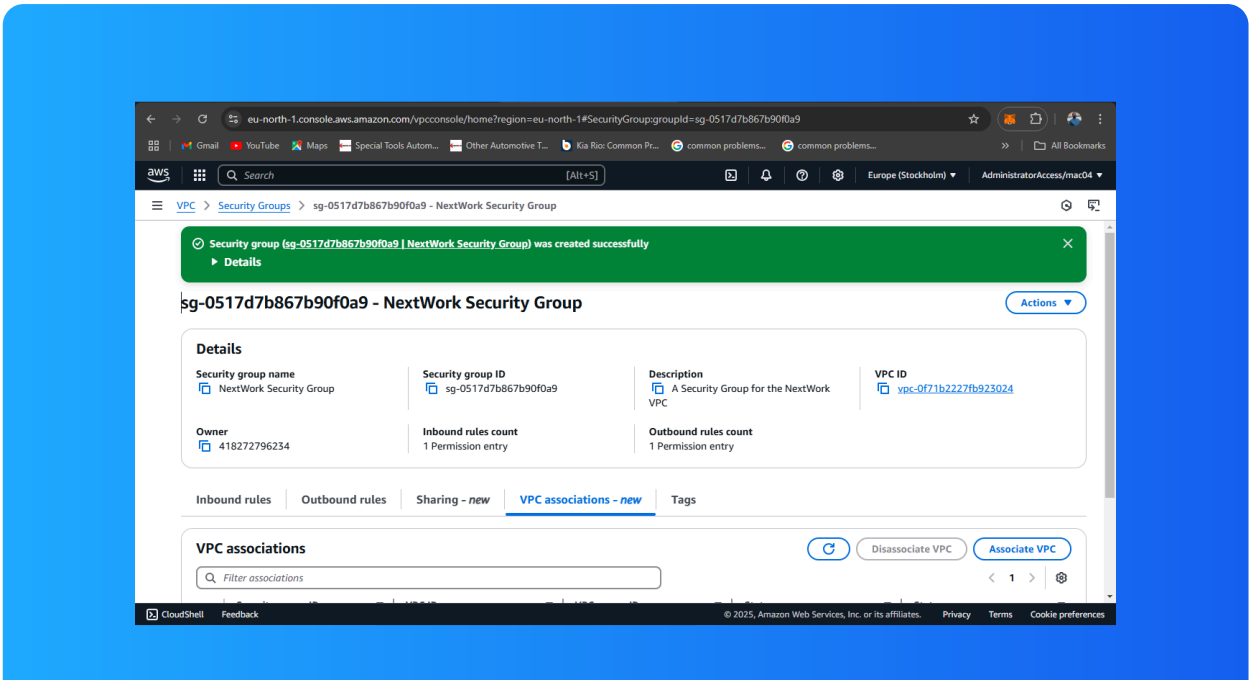
Security groups

Security groups are a means of checkng that only protocols, IP addresses that are allowed, are permitted to interact with the resource within a resources.

Inbound vs Outbound rules

Inbound rules are rules that control the data that can enter resources in the security group. I configured an inbound rule that Type: HTTP and Source: Anywhere-IPv4. This means anyone in the public can access my resource.

Outbound rules are rules that control the data the resources send out. By default, my security group's outbound rule allows my resources to send out data.



Michael Emeruwa
NextWork Student

Network ACLs

Network ACLs are used to set broad traffic rule that apply to entire subnet.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that a Security group is used to control traffic on a granular level, how traffic interacts with a resource, while network ACL controls how traffic interacts with an entire subnet

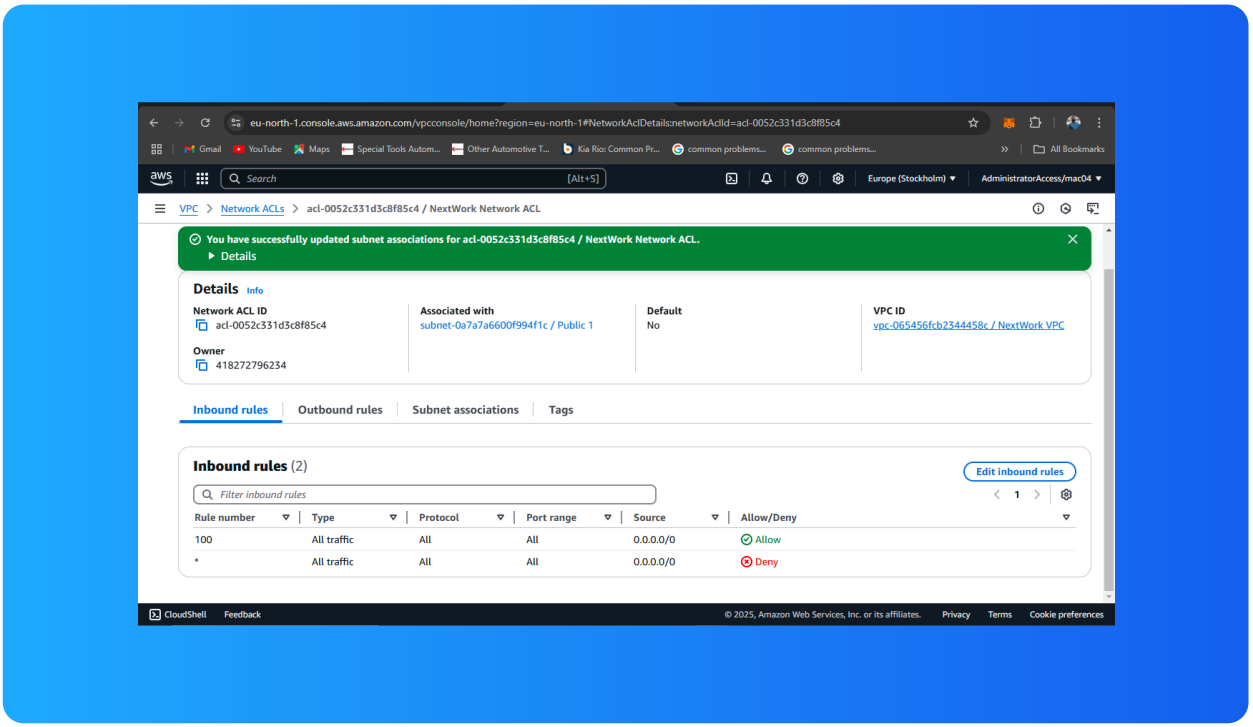
Michael Emeruwa
NextWork Student

Default vs Custom Network ACLs

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

By default, a network ACL's inbound and outbounf rules will allow all traffic to enter and leave the subnet.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic unless customized.



Everyone should be in a job they love.

Check out nextwork.org for more projects