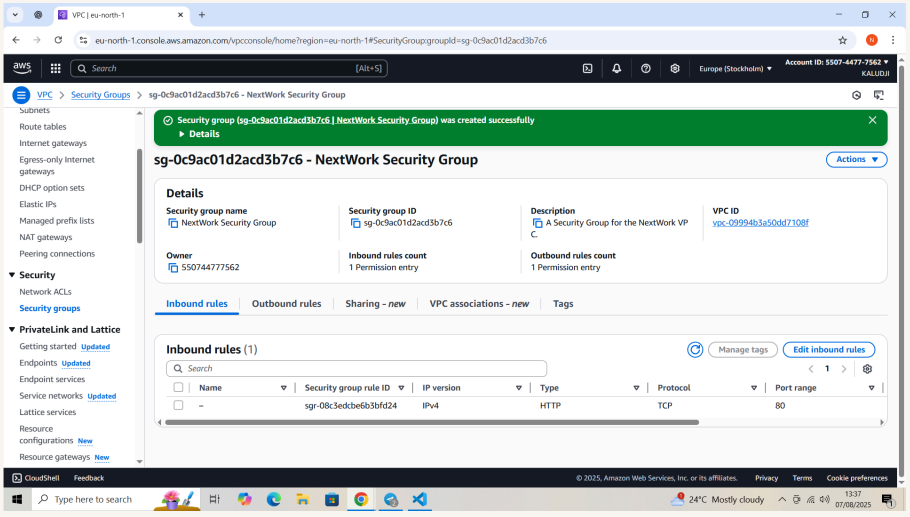
nextwork.org

VPC Traffic Flow and Security

Nchindo Boris



Nchindo Boris
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual network you create inside AWS that’s logically isolated from other networks.It is useful in providing full control over resources in the cloud

How I used Amazon VPC in this project

Amazon VPC was used in today's project to provide an environment for; Subnets Routing Security (via security groups and NACLs) Internet access (via gateways) In order to control traffic flow and security

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

One thing you didn't expect in this project is the substantial amount of security put in place to protect resources in the cloud

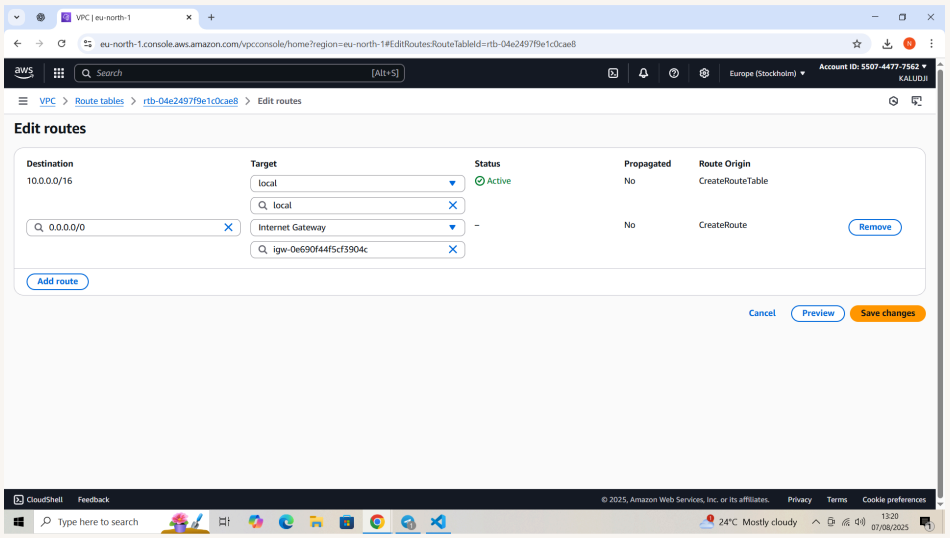
This project took me...

It took me 1 hour 30 minutes to complete this project

Route tables

Route tables are sets of rules (called routes) that determines how network traffic is directed within a Virtual Private Cloud (VPC)

Routes tables are needed to make a subnet public because they define how the traffic flows from your subnet to the internet. A subnet becomes public when its route table has a rule that sends outbound traffic to the Internet Gateway

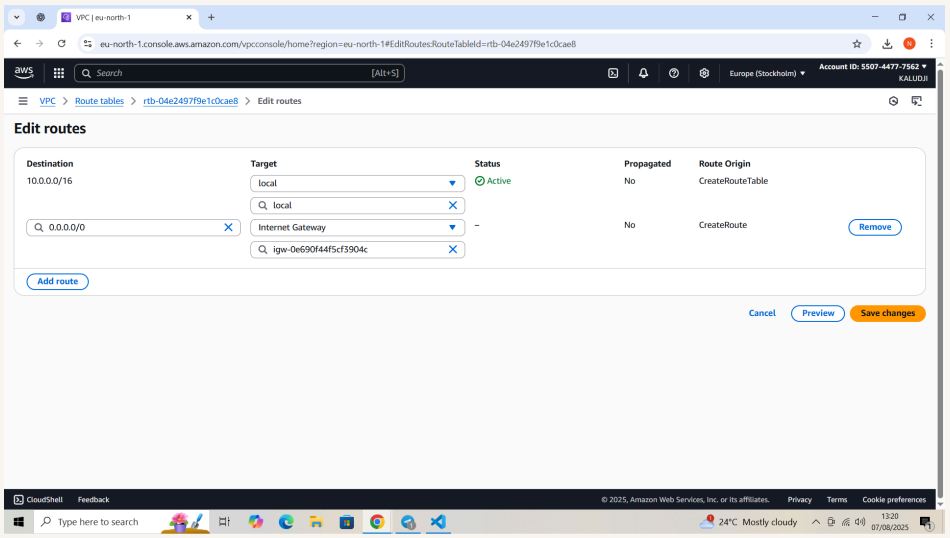


Nchindo Boris
NextWork Student

Route destination and target

Routes are defined by their destination and target, which means 1. Destination This is the IP address range (CIDR block) that defines where traffic is going 2. Target This is the gateway that AWS should use to send traffic to the destination

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 Internet Gateway



Security groups

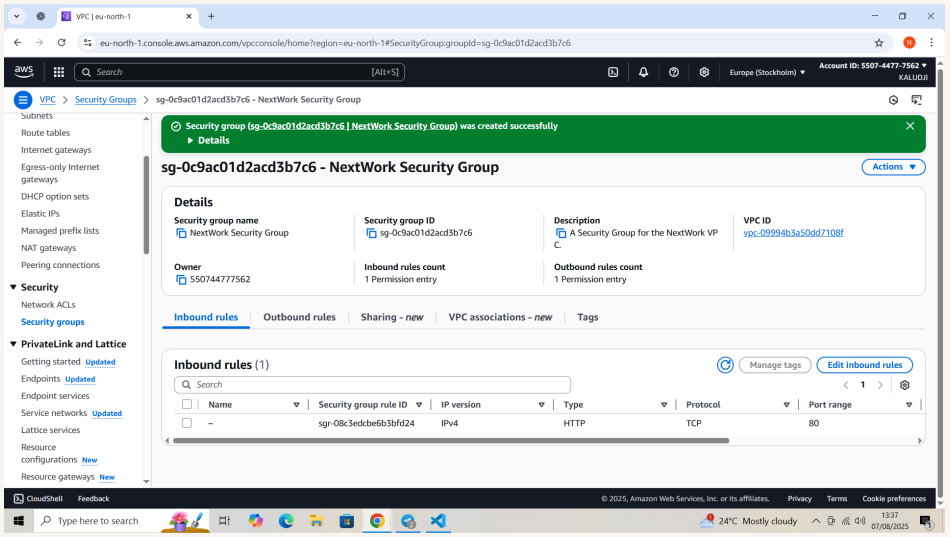
Security groups act like virtual firewalls for your resources. They control inbound and outbound traffic at the instance level, based on rules you define

Inbound vs Outbound rules

An inbound rule defines what kind of incoming traffic is allowed to reach a resource. My security group's inbound rule is Allow HTTP Access from Anyone. This allows anyone to visit a website hosted on my resource

An outbound rule in AWS controls the traffic leaving my resource. My security group's outbound rule is Allow All Outbound Traffic

Nchindo Boris
NextWork Student



Network ACLs

Network ACLs (Access Control Lists) are firewalls that control inbound and outbound traffic to and from entire subnets, based on rules you define.

Security groups vs. network ACLs

Network ACLs are used to set broad traffic rules that apply to an entire subnet. Security groups allow access to individual resources

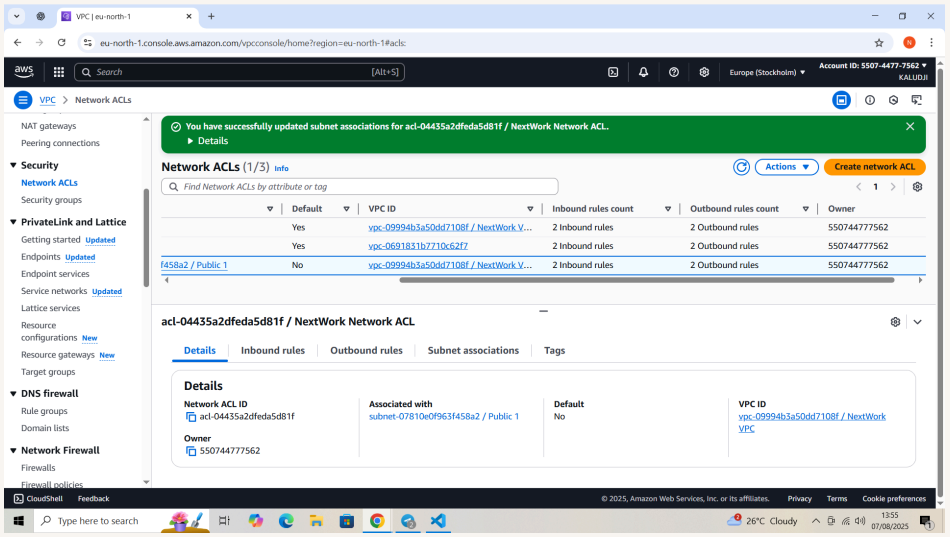
Nchindo Boris
NextWork Student

Default vs Custom Network ACLs

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

By default, a network ACL's inbound and outbound rules will allow all traffic

In contrast, a custom ACL's inbound and outbound rules are automatically set to DENY by default until you add ALLOW rules.



The place to learn & showcase your skills

Check out nextwork.org for more projects