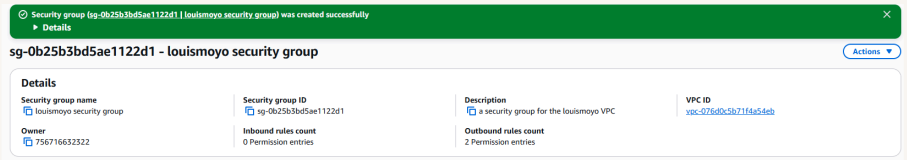
nextwork.org

VPC Traffic Flow and Security

Louis Moyo



Louis Moyo
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private cloud network within AWS. It’s useful because it lets you control IP ranges, subnets, routing, and security for your resources.

How I used Amazon VPC in this project

I used Amazon VPC to create a secure network with subnets, route tables, an internet gateway, and ACLs to host an EC2 instance safely.

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

I didn’t expect how many separate steps and configurations were needed just to make an EC2 instance accessible on the internet securely.

This project took me...

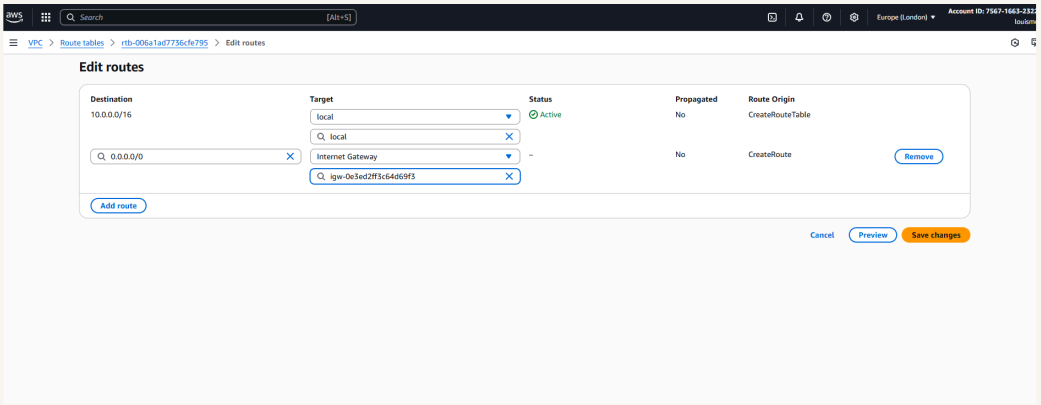
his project took me around 1.5 hours to complete, including setting up the VPC, subnets, routing, security groups, and testing connectivity.

Louis Moyo
NextWork Student

Route tables

Route tables are sets of rules that control where network traffic from your VPC is directed.

Route tables are needed to make a subnet public because they must have a route that sends internet-bound traffic to an internet gateway.

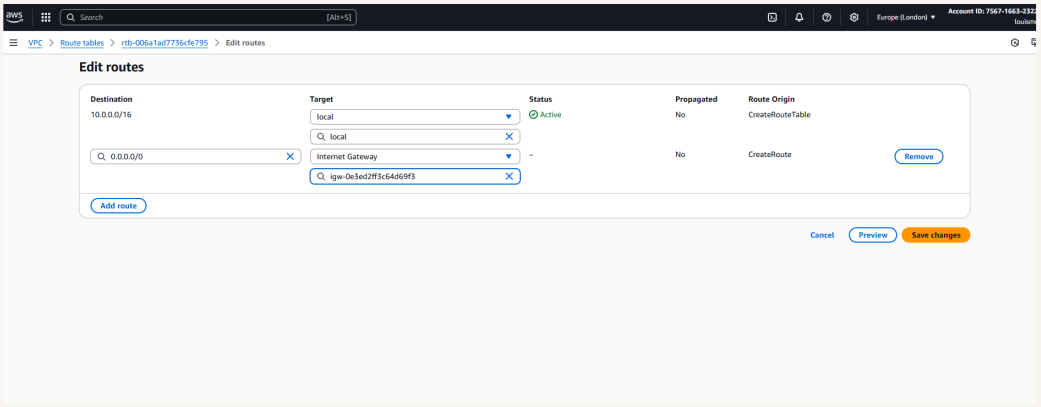


Louis Moyo
NextWork Student

Route destination and target

The destination is where the traffic is going, and the target is the resource that handles that traffic.

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 my internet gateway.



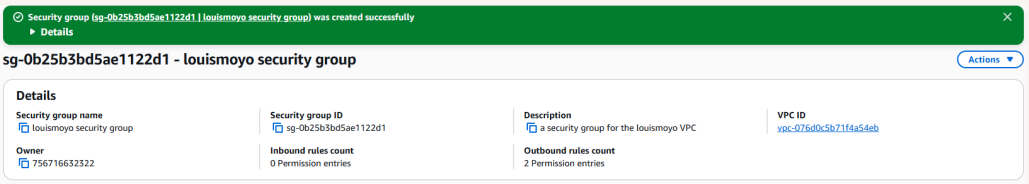
Security groups

Security groups are virtual firewalls for EC2 instances that control inbound and outbound traffic. They allow or deny traffic based on rules you define.

Inbound vs Outbound rules

Inbound rules control what traffic is allowed to enter your resource. I configured an inbound rule that allows SSH (port 22) and HTTP (port 80) from my IP so I can manage and access the instance.

Outbound rules control what traffic can leave your resource. By default, my security group's outbound rule allows all outbound traffic to any destination.


Security group (sg-0b25b3bd5ae1122d1 | louismoyo security group) was created successfully
Details
sg-0b25b3bd5ae1122d1 - louismoyo security group
Actions
Details
Security group name
louismoyo security group
Security group ID
sg-0b25b3bd5ae1122d1
Description
a security group for the louismoyo VPC
VPC ID
vpc-076d0c5b71f4a54eb
Owner
756716632322
Inbound rules count
0 Permission entries
Outbound rules count
2 Permission entries

L
Louis Moyo
NextWork Student

Network ACLs

Network ACLs are subnet-level firewalls that control inbound/outbound traffic using rules to allow or deny based on IPs, ports, and protocols. They are stateless.

Security groups vs. network ACLs

Security groups are instance-level and stateful, return traffic is auto-allowed. NACLs are subnet-level and stateless, return traffic must be explicitly allowed.

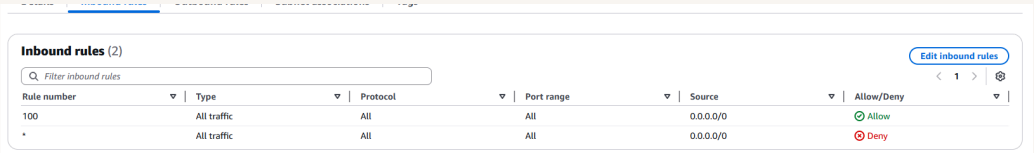
Louis Moyo
NextWork Student

Default vs Custom Network ACLs

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

By default, a network ACL allows all inbound and outbound traffic for the subnets it's associated with.

A new custom NACL denies all inbound and outbound traffic until rules are added to explicitly allow it.



The place to learn & showcase your skills

Check out nextwork.org for more projects