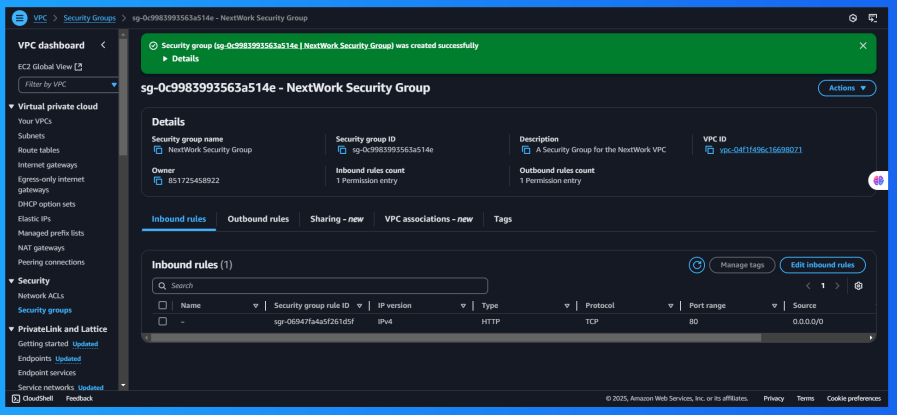
NextWork.org

VPC Traffic Flow and Security

Honesty Dogunro



H
Honesty Dogunro
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you create a secure, isolated space in AWS for your resources, enabling control over network settings and enhancing security.

How I used Amazon VPC in this project

I used Amazon VPC to set up a secure network for our application, defining subnets, route tables, and security groups to control access and ensure data protection. This isolated environment enhanced our project's security and performance.

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

I didn't expect the complexity of configuring security groups to manage access effectively.

This project took me...

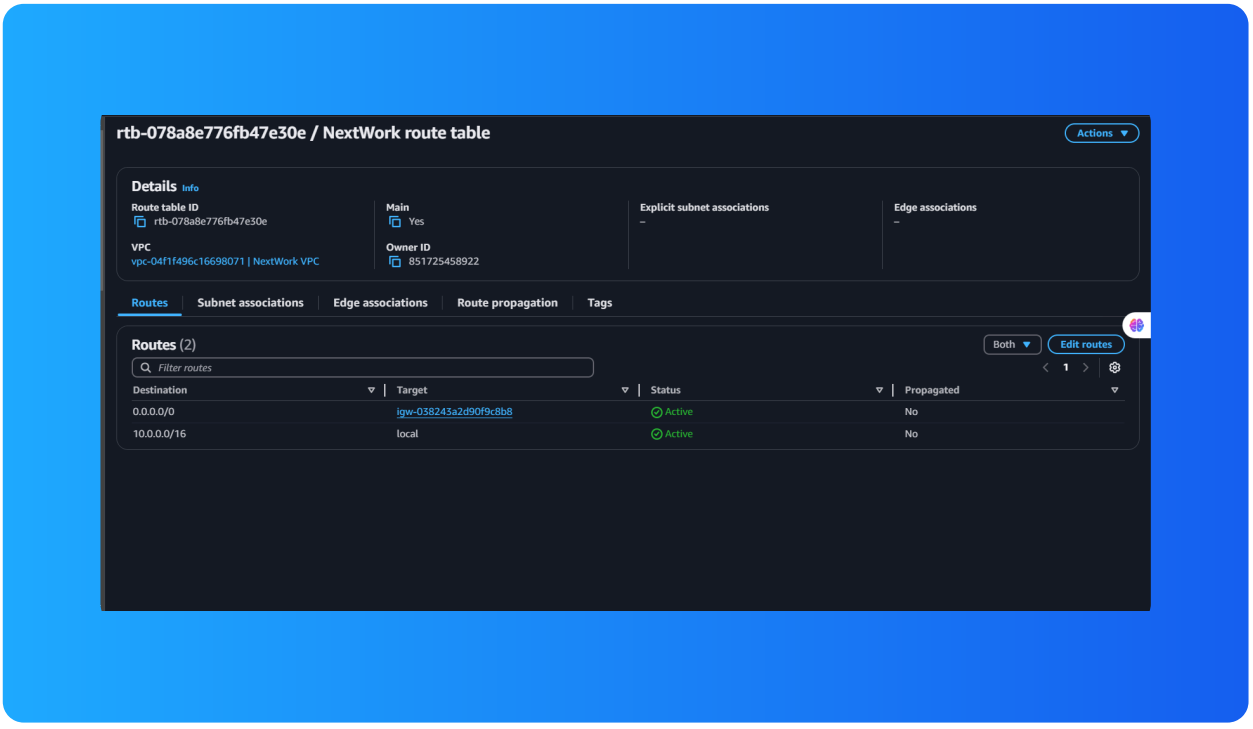
About 3 hours, i needed to understand those network concepts and configurations

H
Honesty Dogunro
NextWork Student

Route tables

Route tables are lists of rules in networking that direct data packets between networks.They include destination IPs,subnet masks,next hops,and metrics to determine the best path for traffic,ensuring efficient communication and reliable data delivery

Route tables are needed to make a subnet public because they direct traffic between the subnet and the internet, allowing external access through an internet gateway.

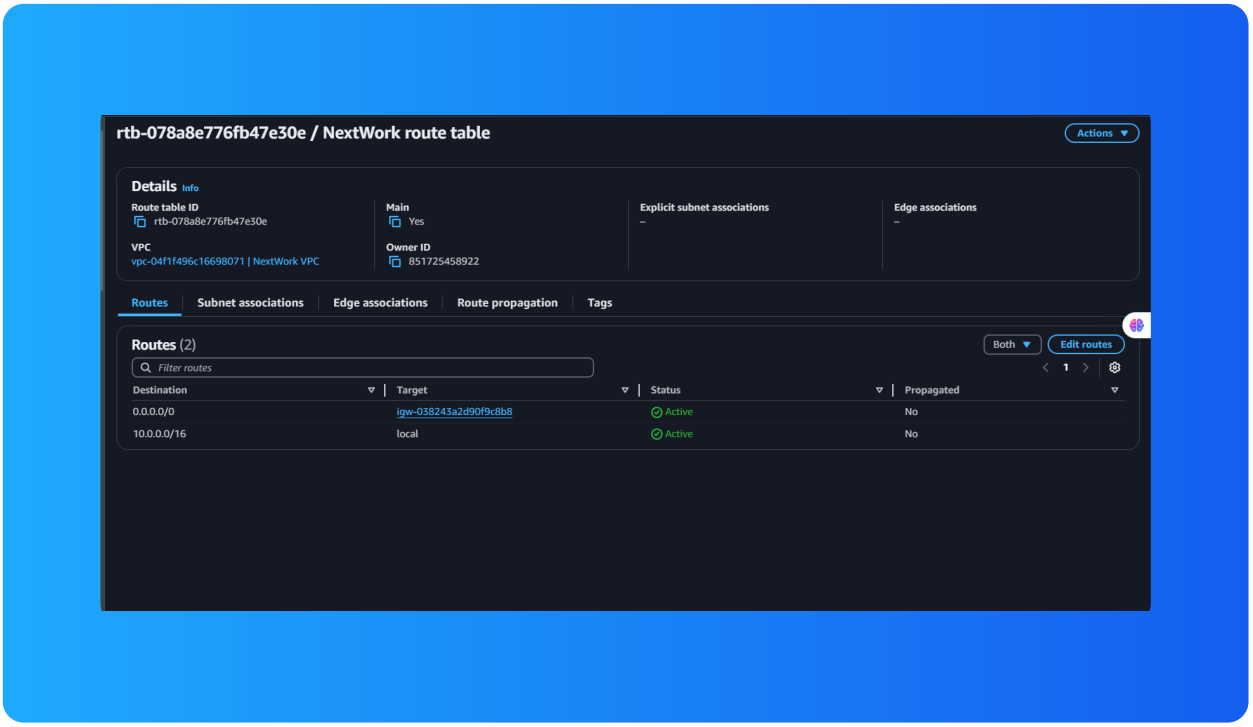


Honesty Dogunro
NextWork Student

Route destination and target

Routes are defined by their destination and target, which means the destination specifies the IP range being reached, while the target indicates where the traffic should go next, often a next-hop IP address or a gateway for forwarding packets.

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 the internet gateway's ID (e.g. igw-12345678).



Honesty Dogunro
NextWork Student

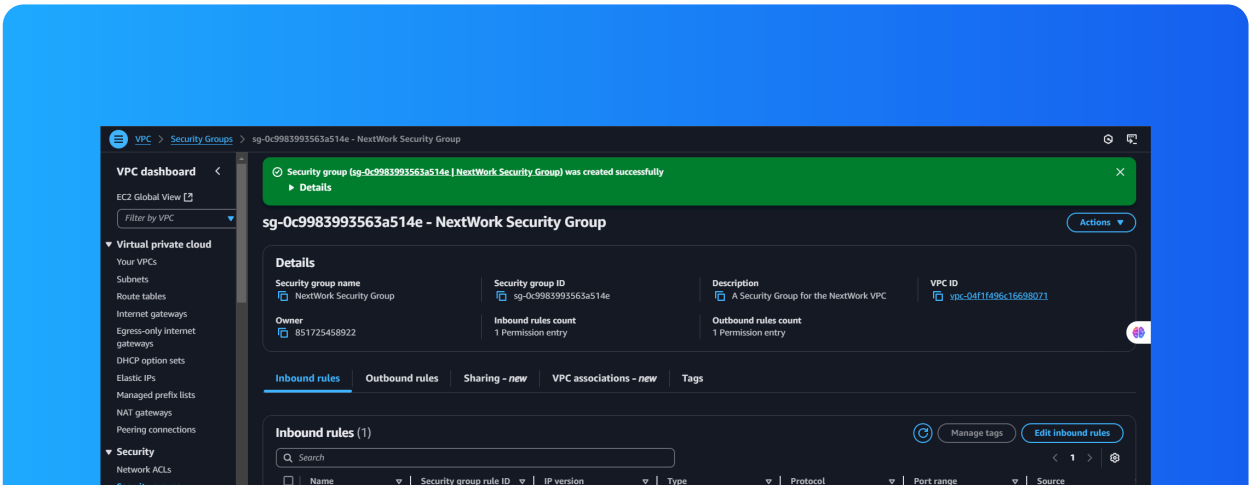
Security groups

Security groups are virtual firewalls in cloud computing that control inbound and outbound traffic to resources, like EC2 instances. They define which protocols and ports are allowed, helping to secure applications and manage access effectively.

Inbound vs Outbound rules

Inbound rules are the guidelines that determine which incoming traffic is allowed to reach your resources within a security group. I configured an inbound rule that permits HTTP traffic on port 80 from any IP address to allow web access.

Outbound rules are the guidelines that control the outgoing traffic from your resources within a security group. By default, my security group's outbound rule allows all traffic to any IP address, enabling free communication to the internet.



H
Honesty Dogunro
NextWork Student

Network ACLs

Network ACLs are access control lists used in networking to define rules that govern incoming and outgoing traffic at the subnet level within a virtual private cloud (VPC). They enhance security by filtering traffic based on IP addresses and protocol

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are stateful and apply to instances, while network ACLs are stateless and apply to subnets, requiring explicit rules for both inbound and outbound traffic.

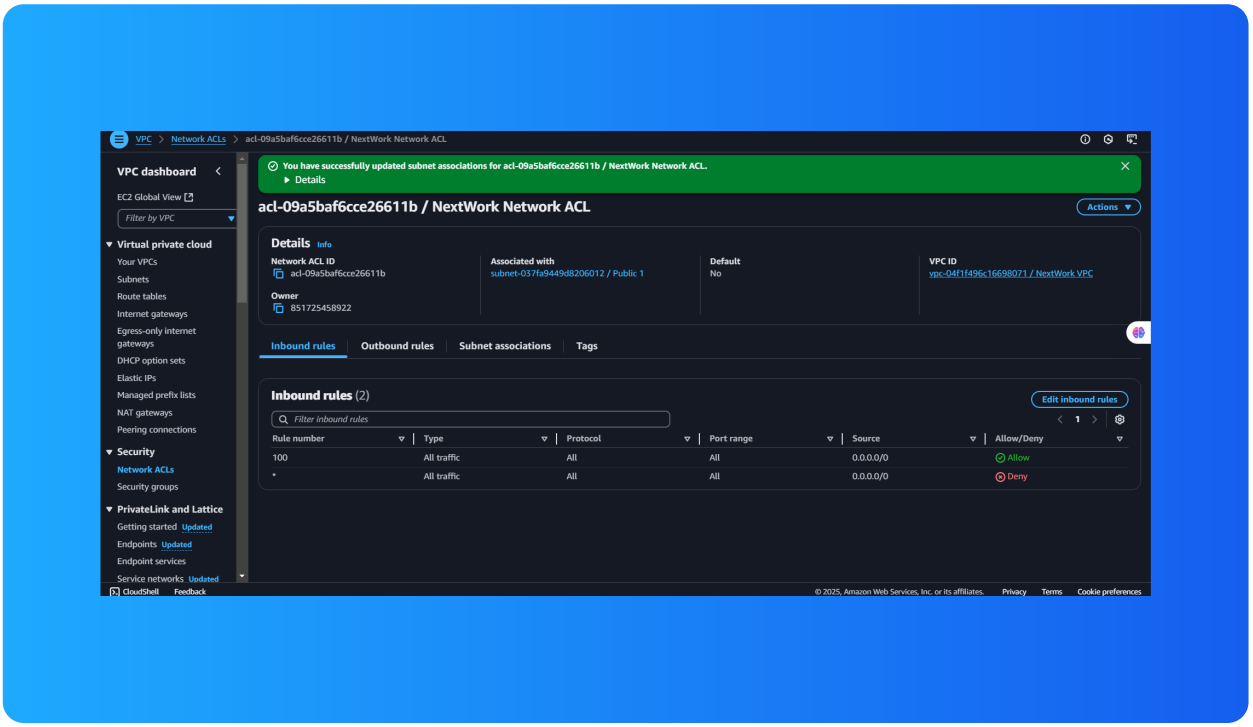
Honesty Dogunro
NextWork Student

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, meaning they have an implicit rule that permits all IP traffic unless explicitly denied. This ensures that all connections are allowed by default.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic until explicitly allowed, meaning you must define rules to permit specific traffic based on IP addresses, protocols, and ports.



Everyone should be in a job they love.

Check out nextwork.org for more projects