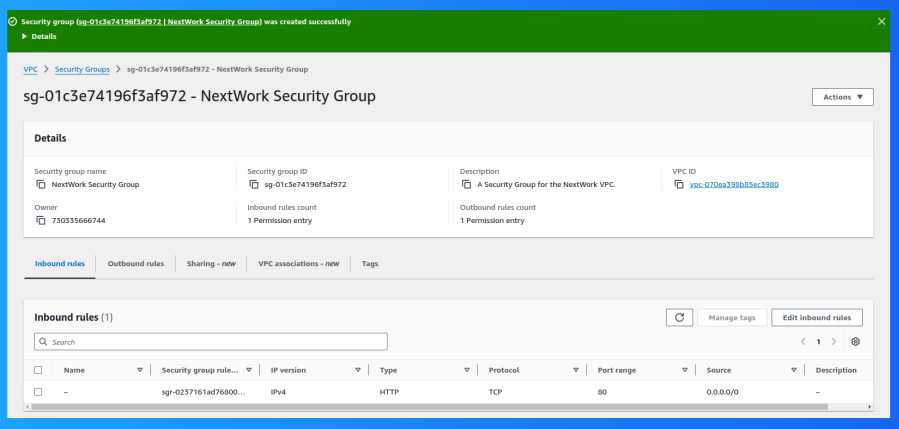
NextWork.org

VPC Traffic Flow and Security

Emmanuel Enalpe III



Emmanuel Enalpe III
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you create a private network within AWS to securely launch and manage resources. It’s useful for controlling traffic, improving security, and isolating workloads, ensuring a customized network environment.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a secure network environment for deploying resources, ensuring isolated communication between services, and controlling access with security groups and subnet configurations.

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

I didn't expect the simplicity, but it has a lot of configurations to do in order to setup a secured VPC.

This project took me...

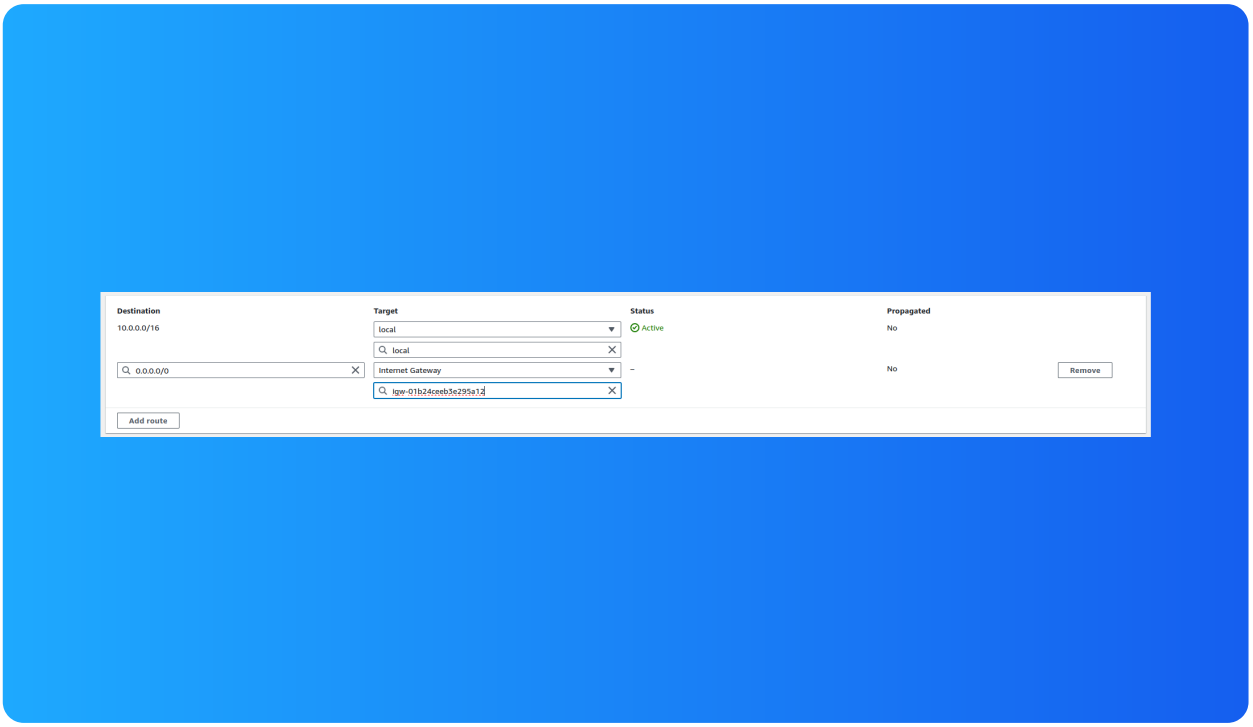
I took me an less than an hour to complete this project.

Emmanuel Enalpe III
NextWork Student

Route tables

Route tables are resources in a VPC that direct traffic to destinations based on rules, determining how data flows between subnets, internet gateways, NAT gateways, or other network resources.

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

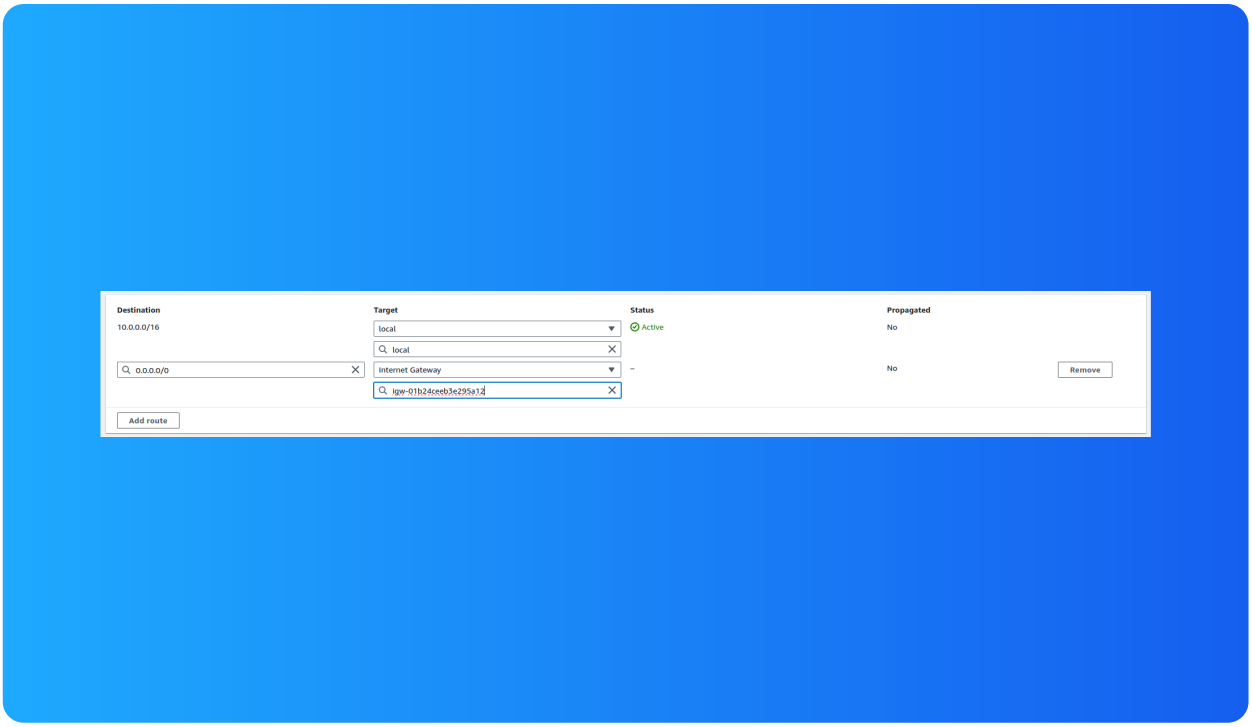


Emmanuel Enalpe III
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the destination specifies the traffic's endpoint (e.g., IP or CIDR), and the target is the resource (e.g., internet gateway, NAT, instance) forwarding the 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 the internet gateway (igw-xxxxxxxx).



Emmanuel Enalpe III
NextWork Student

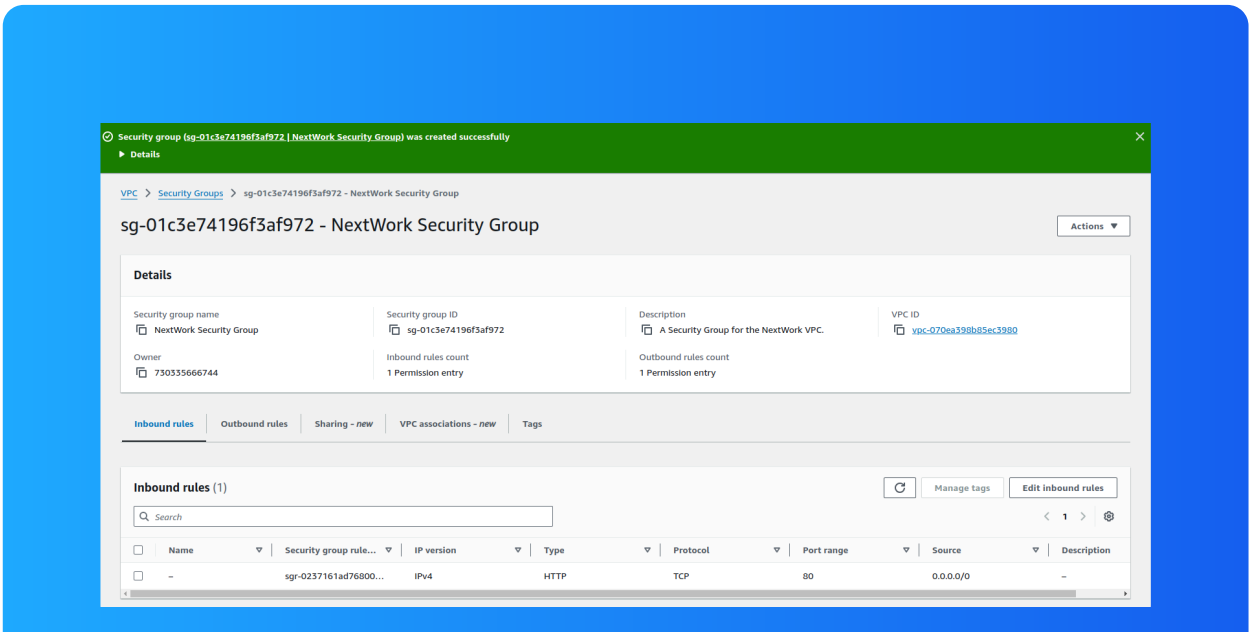
Security groups

Security groups are virtual firewalls in AWS that control inbound and outbound traffic to resources like EC2 instances. They define rules based on IP address, protocol, and port, ensuring secure access to the resources.

Inbound vs Outbound rules

Inbound rules are security group settings that control incoming traffic to your resources. I configured an inbound rule that allows HTTP traffic on port 80 from any IP address to enable web access to my server.

Outbound rules are configurations that control the traffic leaving a security group. By default, my security group's outbound rule allows all outbound traffic, meaning it permits all traffic to leave the instances without restriction.



Emmanuel Enalpe III
NextWork Student

Network ACLs

Network ACLs are a set of rules that control inbound and outbound traffic to and from a subnet in a VPC. They provide an additional layer of security by allowing or denying traffic based on IP addresses and port numbers.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups act as virtual firewalls for EC2 instances, controlling inbound and outbound traffic, while network ACLs control traffic at the subnet level with stateless filtering.

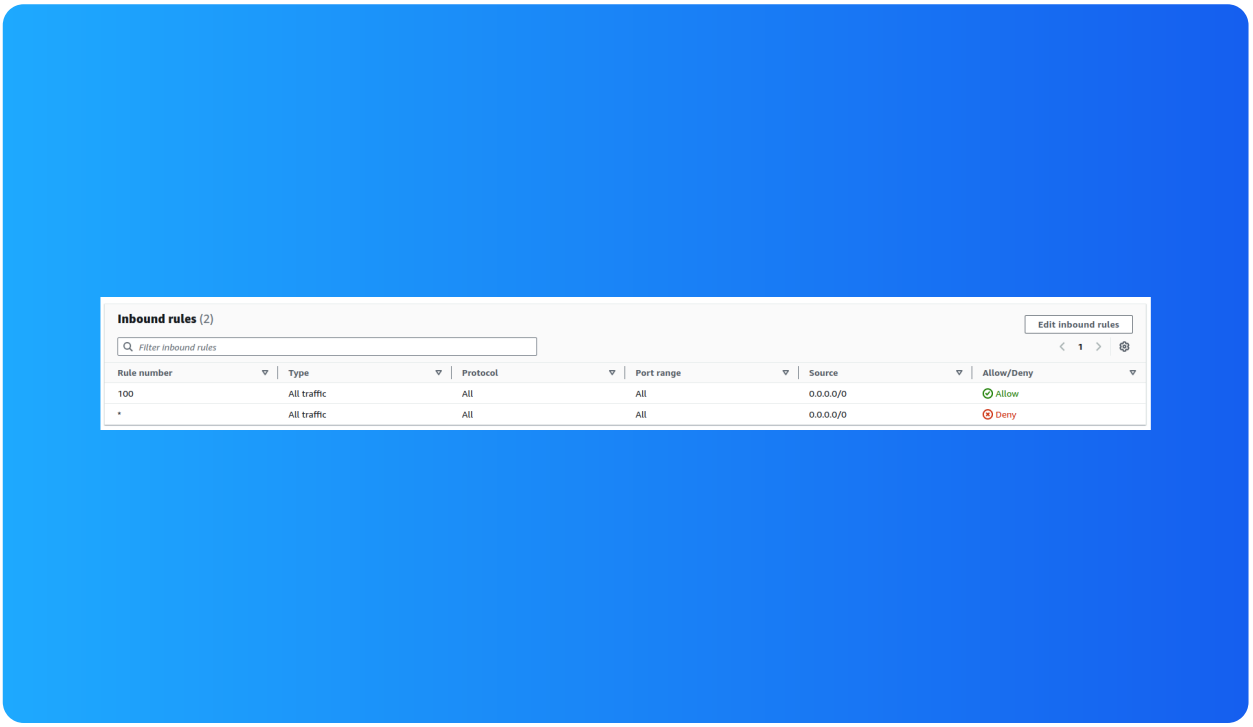
Emmanuel Enalpe III
NextWork Student

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 (allow all inbound and outbound traffic) and deny no traffic by default, providing unrestricted communication unless modified.

In contrast, a custom ACL's inbound and outbound rules are automatically set to allow all traffic by default. You can modify these rules to specify which traffic is allowed or denied based on IP address, protocol, and port.



Everyone should be in a job they love.

Check out nextwork.org for more projects