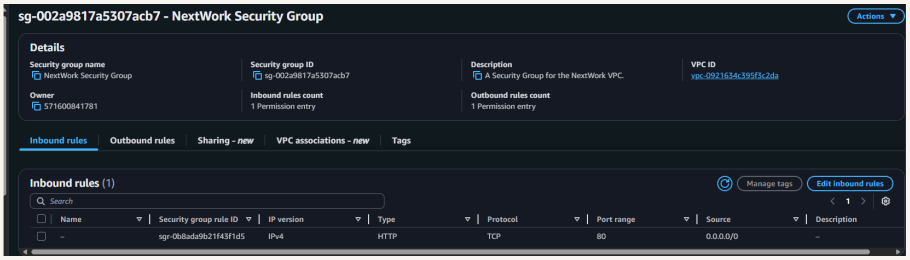
nextwork.org

VPC Traffic Flow and Security

Coran Chunilall



Coran Chunilall
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual private cloud that creates an isolated network within AWS. It's useful because it provides secure, customizable networking with control over IP ranges, subnets, routing, and security for your AWS resources.

How I used Amazon VPC in this project

We used a VPC to connect to a Route table , security groups and NACL

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

I did not expect to configure a Security group

This project took me...

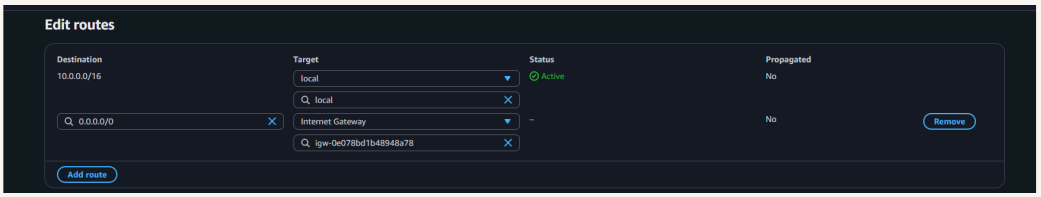
1 hour

Coran Chunilall
NextWork Student

Route tables

Route tables are networking components that direct traffic between network segments. They contain rules specifying where packets should go based on destination IPs, including next hop routers and interfaces for optimal routing.

Route tables are needed to make a subnet public because they contain routes directing traffic to an internet gateway. Without a route (like 0.0.0.0/0 → IGW), instances can't reach the internet even if an IGW exists.

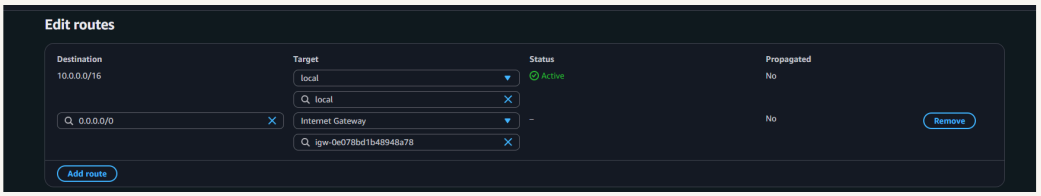


Coran Chunilall
NextWork Student

Route destination and target

Routes are defined by their destination and target, which means the destination specifies which traffic the route applies to (like 0.0.0.0/0 for all internet traffic), while the target defines where that traffic should be sent to a internet gateway

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



Coran Chunilall
NextWork Student

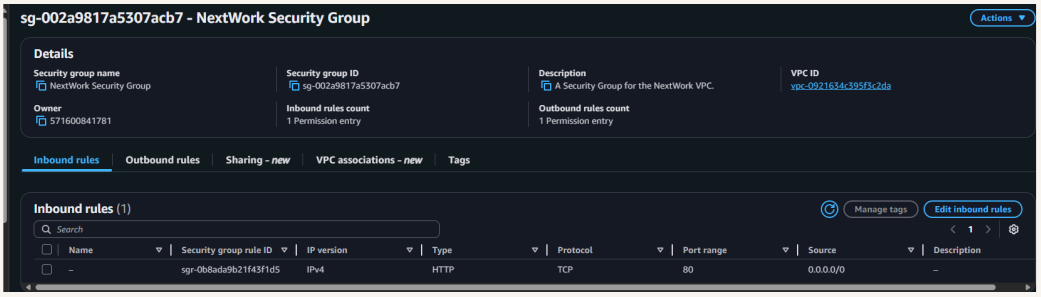
Security groups

Security groups are virtual firewalls that control inbound and outbound traffic at the instance level. They're stateful, meaning return traffic is automatically allowed, and operate on allow-only rules, denying all traffic except what's allowed

Inbound vs Outbound rules

Inbound rules control the data that can enter the resources in your security group. I configured an inbound rule that allow HTTP traffic from "0.0.0.0/0" (meaning any IP address) is typical and necessary for public subnets

Outbound rules control that data that your resources can send out. By default my security groups outbound rule is 0.0.0.0/0


sg-002a9817a5307acb7 - NextWork Security Group
Actions
Details
Security group name
NextWork Security Group
Security group ID
sg-002a9817a5307acb7
Description
A Security Group for the NextWork VPC.
VPC ID
vpc-0921634c395f3c2da
Owner
571600841781
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags
Inbound rules (1)
Manage tags
Edit inbound rules
Search
Name
Security group rule ID
IP version
Type
Protocol
Port range
Source
Description
–
sgr-0b8ada9b21f43f1d5
IPv4
HTTP
TCP
80
0.0.0.0/0
–

Coran Chunilall
NextWork Student

Network ACLs

Network ACLs are used to set broad traffic rules that apply to an entire subnet

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are stateful instance-level firewalls with allow-only rules, while NACLs are stateless subnet-level firewalls with both allow/deny rules processed in order.

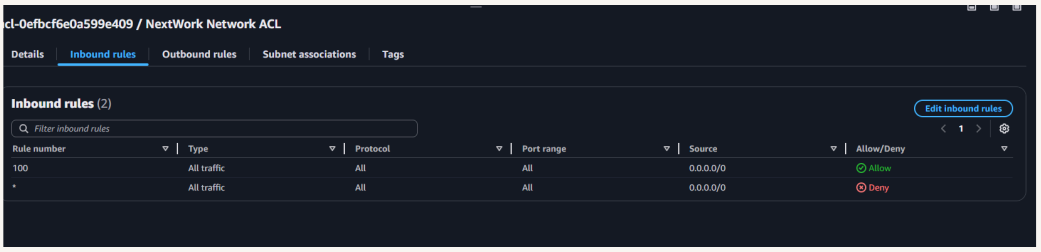
Coran Chunilall
NextWork Student

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 deny all traffic

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic. Custom NACLs start with explicit deny rules (DENY ALL) for both inbound and outbound traffic, requiring you to manually add allow rules for any traffic



The place to learn & showcase your skills

Check out nextwork.org for more projects