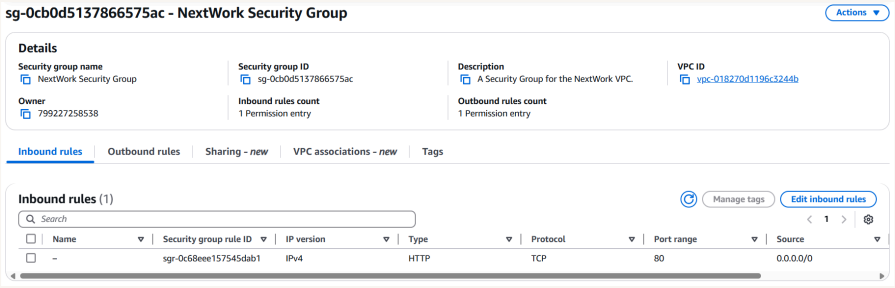
nextwork.org

VPC Traffic Flow and Security

MHM Aslam



MHM Aslam
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC lets you create a private network in AWS, giving full control over IP ranges, subnets, and routing. It's useful for securely launching resources, managing traffic, and customizing your cloud environment to fit specific needs.

How I used Amazon VPC in this project

I used Amazon VPC in today’s project to create a secure network, set up subnets, attach an internet gateway, and configure security groups. This allowed my resources to connect to the internet and communicate safely within the VPC.

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

One thing I didn't expect in this project was how many small but important steps—like enabling auto-assign public IPs or setting up correct inbound rules were required to make everything work as expected. Missing one could block all access.

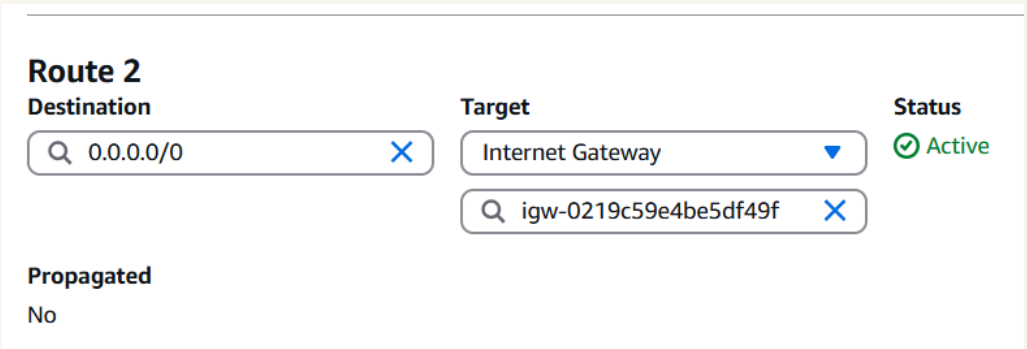
This project took me...

This project took me around 2 hours to learn and apply the concepts, setting up the VPC, subnets, and internet gateway while configuring key settings to ensure everything worked smoothly.

Route tables

Route tables are rules in a VPC that control where network traffic is directed. They determine how data moves between subnets, the internet, and other networks. Each subnet must be associated with a route table to send traffic properly.

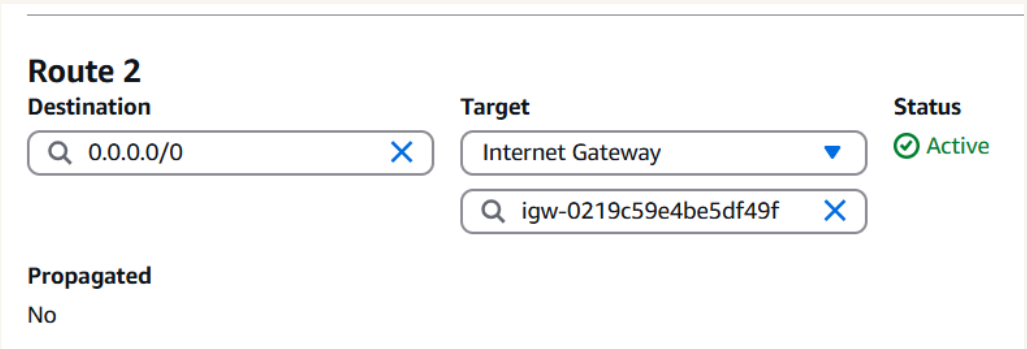
Route tables are needed to make a subnet public because they define a route to the internet through an internet gateway. Without this route, even with a public IP, instances can't send or receive traffic from the internet.



Route destination and target

Routes are defined by their destination and target, which mean the destination is the IP range the traffic is meant for, and the target is the resource (like an internet gateway) that handles forwarding 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 named NextWork IG.



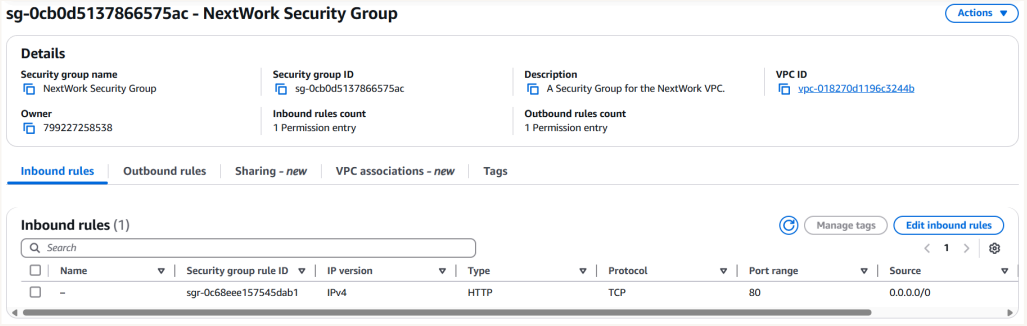
Security groups

Security groups are virtual firewalls that control inbound and outbound traffic to AWS resources, like EC2 instances. They act as filters, allowing or blocking traffic based on defined rules for protocols, ports, and IP addresses.

Inbound vs Outbound rules

Inbound rules are settings that control the traffic allowed to enter your resources. I configured an inbound rule that allows HTTP traffic on port 80 from Anywhere-IPv4, meaning any IPv4 address can access my web server.

Outbound rules are settings that control the traffic allowed to leave your resources. By default, my security group's outbound rule allows all traffic to any destination, letting instances communicate freely with the internet and other networks.


sg-0cb0d5137866575ac - NextWork Security Group
Actions
Details
Security group name
NextWork Security Group
Security group ID
sg-0cb0d5137866575ac
Description
A Security Group for the NextWork VPC.
VPC ID
vpc-018270d1196c3244b
Owner
799227258538
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
1
Name
Security group rule ID
IP version
Type
Protocol
Port range
Source
–
sgr-0c68eee157545dab1
IPv4
HTTP
TCP
80
0.0.0.0/0


MHM Aslam
NextWork Student

Network ACLs

Network ACLs are stateless firewalls at the subnet level that control inbound and outbound traffic using numbered rules. They allow or deny traffic based on IP, protocol, and port, and apply to all resources within the subnet.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups secure resources at the instance level and are stateful, while network ACLs secure traffic at the subnet level and are stateless, needing rules for both directions.

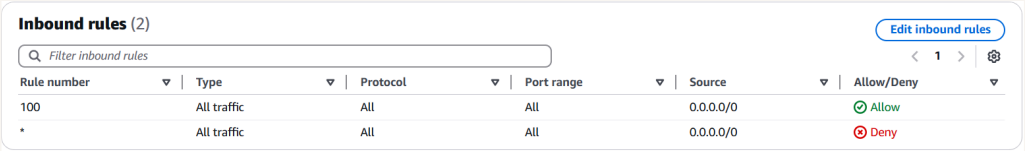
MHM Aslam
NextWork Student

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 and out. This means all protocols, ports, and IPs are permitted unless you modify the rules to restrict specific traffic.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic. You must manually add rules to allow specific traffic through the subnet.



The place to learn & showcase your skills

Check out nextwork.org for more projects