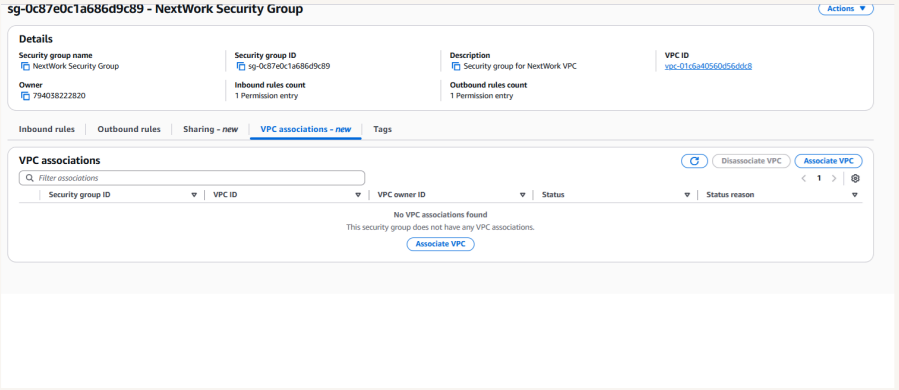
nextwork.org

VPC Traffic Flow and Security

Sanjana Tripathy



Sanjana Tripathy
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private network in AWS where you can launch resources securely. It lets you control IP ranges, subnets, routing, and access using internet gateways, route tables, security groups, and network ACLs for secure communication.

How I used Amazon VPC in this project

In today's project,I used Amazon VPC to create a custom virtual network.I added subnets, attached an internet gateway,set up a route table for internet access, and applied security groups and network ACLs to control traffic and secure the environment

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

What I didn’t expect in this project was the depth and range of topics involved. However, exploring each component—from subnets to security layers—made the experience both insightful and enriching, strengthening my understanding of AWS networking.

This project took me...

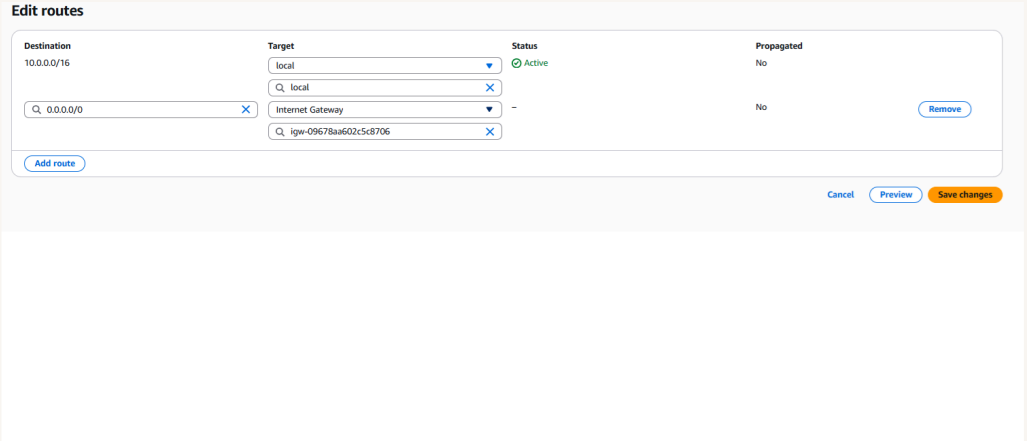
This project took me approximately 3 to 5 hours to complete, as it covered a wide range of topics. Exploring each concept in depth—like subnets, route tables, and security layers—took time but greatly enhanced my understanding.

Sanjana Tripathy
NextWork Student

Route tables

Route tables in AWS are a set of rules that control where network traffic is directed. Each subnet in a VPC is linked to a route table, which uses destination IPs and targets (like IGW or local) to determine the traffic's next hop.

You need a route table to make a subnet public because it must have a rule that sends traffic destined for the internet (0.0.0.0/0) to an Internet Gateway (IGW). Without this route, resources in the subnet can't reach the internet.

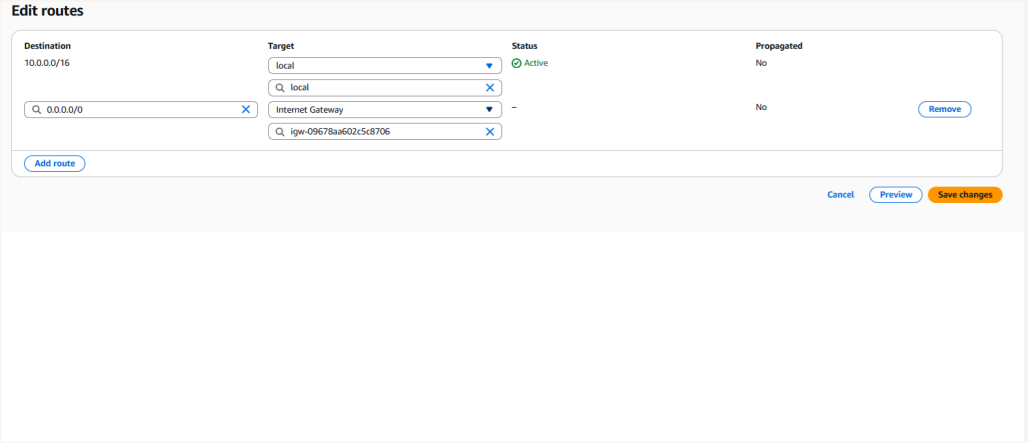


Sanjana Tripathy
NextWork Student

Route destination and target

In a route,the destination is the IP range the traffic wants to reach (like 0.0.0.0/0 for internet or 10.0.0.0/16 for internal VPC).The target is the path the traffic takes to get there, like an Internet Gateway or local for VPC-internal routing.

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 igw.



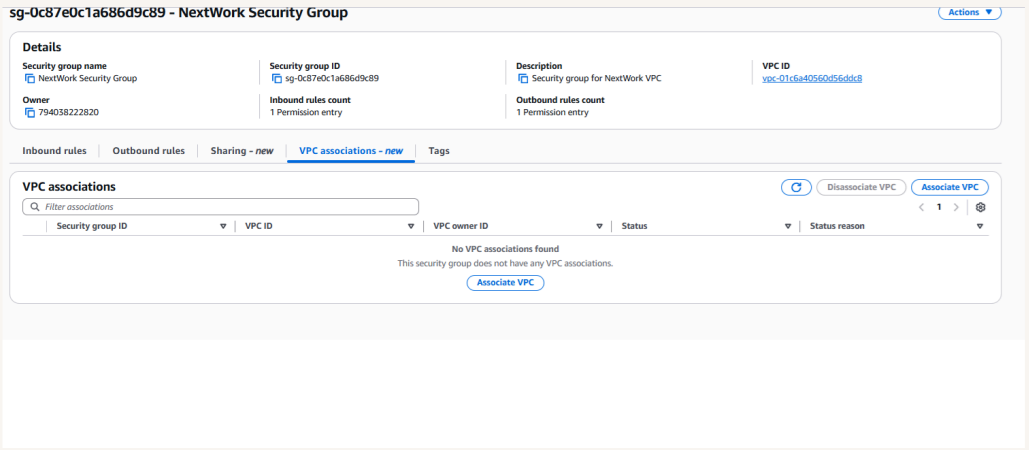
Security groups

Security groups are virtual firewalls in AWS that control inbound and outbound traffic for resources like EC2. You define rules based on IP, port, and protocol. By default, all inbound is denied, and outbound is allowed.

Inbound vs Outbound rules

Inbound rules control the traffic that is allowed to enter a AWS resource from the outside. a user can define which IP, port, and protocol can access it.I configured an inbound rule that that allows all HTTP traffic from any IP address(0.0.0.0/0)

Outbound rules allow specific traffic to leave your AWS resource.By default, my security group's outbound rule state that it allows all outbound traffic.any resource associated with the security group can access and send data to any IP address.


sg-0c87e0c1a686d9c89 - NextWork Security Group
Actions
Details
Security group name
NextWork Security Group
Security group ID
sg-0c87e0c1a686d9c89
Description
Security group for NextWork VPC
VPC ID
vpc-01c6a40560d56ddc8
Owner
794038222820
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags
VPC associations
Disassociate VPC
Associate VPC
Filter associations
1
Security group ID
VPC ID
VPC owner ID
Status
Status reason
No VPC associations found
This security group does not have any VPC associations.
Associate VPC


Sanjana Tripathy
NextWork Student

Network ACLs

Network ACLs (Access Control Lists) are stateless firewalls at the subnet level in AWS. They control inbound and outbound traffic using allow and deny rules based on IP, port, and protocol. Unlike security groups, rules are evaluated in order.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups work at the resource level and are stateful, while network ACLs work at the subnet level and are stateless, requiring separate rules for inbound and outbound traffic.

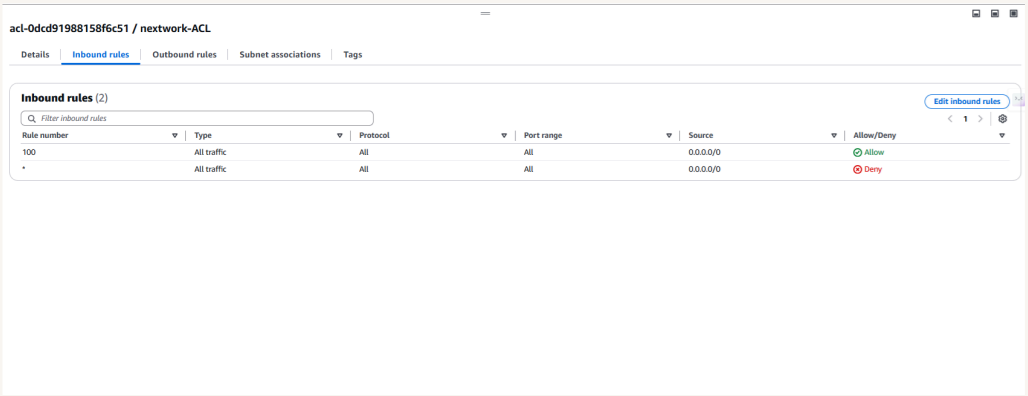
Sanjana Tripathy
NextWork Student

Default vs Custom Network ACLs

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

By default, a network ACL in the default VPC allows all inbound and outbound traffic.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic, requiring you to manually add allow rules.



The place to learn & showcase your skills

Check out nextwork.org for more projects