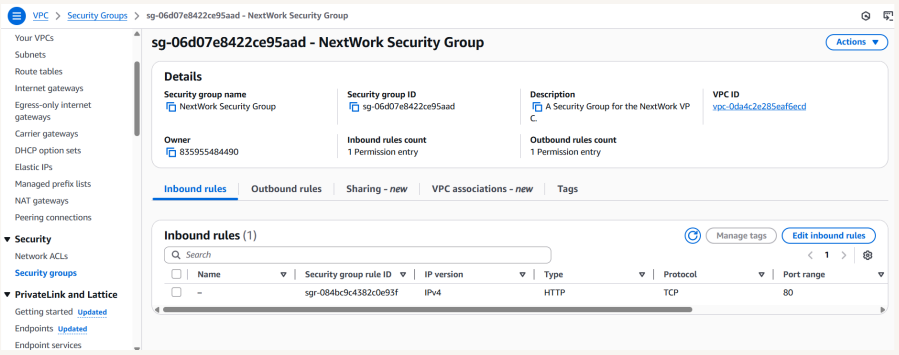
nextwork.org

VPC Traffic Flow and Security

TA Lawrence T. Maguranye



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC lets you create a private network within AWS where you control IP addresses, subnets, routing, and security. It’s useful for securely hosting resources like EC2 instances and databases, with full control over traffic flow and access.

How I used Amazon VPC in this project

I used Amazon VPC to set up a secure network with a public subnet, routing, and access controls—perfect for organizing my project into isolated, manageable layers.

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

One thing I didn't expect in this project was how easily a small routing misconfiguration could block access between tiers—it was a great reminder that in cloud networking, even tiny details matter.

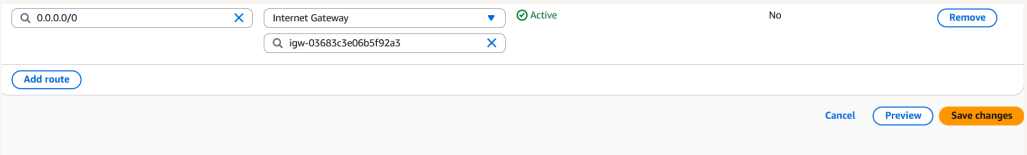
This project took me...

I took me about 2 hours to complete this task.

Route tables

It is a set of rules, called routes, used to determine where network traffic is directed. They are associated with subnets in a VPC and play a key role in controlling the flow of traffic within your cloud network and between the internet.

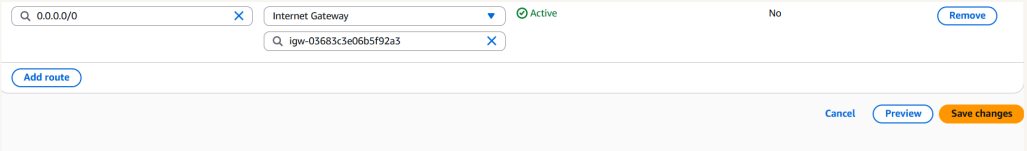
Routes tables are needed to make a subnet public because a subnet becomes public in AWS only when its route table contains a route to the Internet Gateway (IGW). Without this route, resources in the subnet cannot communicate with the internet.



Route destination and target

Routes are defined by their destination and target, which means the destination specifies the range of IP addresses the traffic is intended for, and the target is the gateway through which that traffic should be directed to reach its destination.

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-03683c3e06b5f92a3.



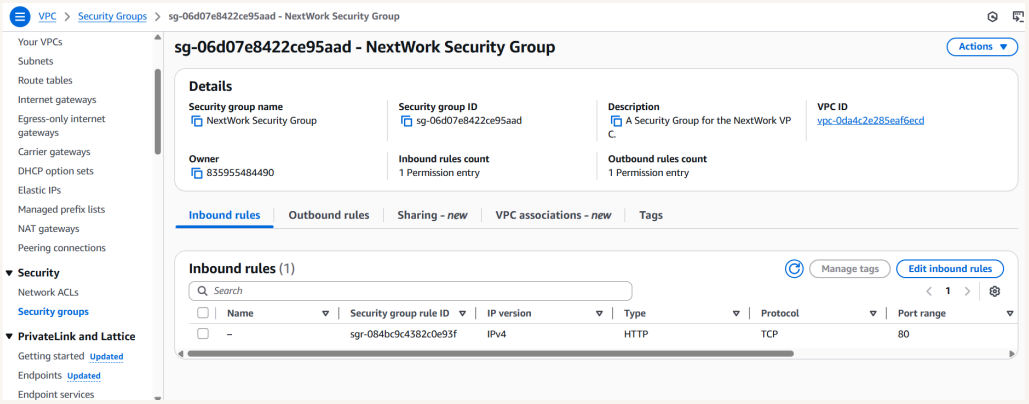
Security groups

Security groups are virtual firewalls in AWS that control inbound and outbound traffic for resources like EC2 instances. They act as gatekeepers, allowing or denying traffic based on rules you define.

Inbound vs Outbound rules

Inbound rules are access control settings that define which incoming traffic is allowed to reach an AWS resource, such as an EC2 instance. I configured an inbound rule that allows all inbound HTTP traffic.

Outbound rules are settings that control which types of traffic your AWS instance is allowed to send out to the internet or other network destinations. By default, my security group's outbound rule will allow all outbound traffic.


VPC > Security Groups > sg-06d07e8422ce95aad - NextWork Security Group
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
PrivateLink and Lattice
Getting started Updated
Endpoints Updated
Endpoint services
sg-06d07e8422ce95aad - NextWork Security Group
Actions
Details
Security group name
NextWork Security Group
Security group ID
sg-06d07e8422ce95aad
Description
A Security Group for the NextWork VPC
VPC ID
vpc-0da4c2e285eaf6ecd
Owner
835955484490
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
–
sgr-084bc9c4382c0e93f
IPv4
HTTP
TCP
80

Network ACLs

Network ACLs are stateless, subnet-level firewalls in AWS that control inbound and outbound traffic in and out of your Virtual Private Cloud (VPC). Network ACLs evaluate every request independently—both coming in and going out.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are stateful and operate at the instance level, while network ACLs are stateless and work at the subnet level.

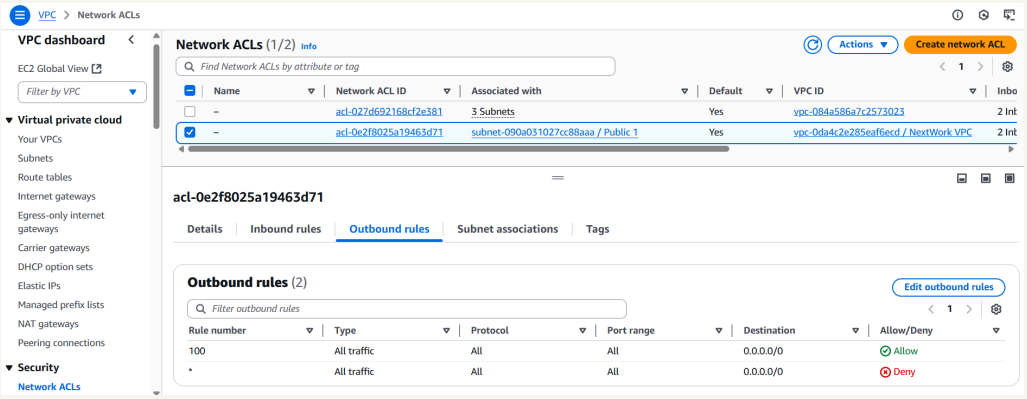
TA
Lawrence T. Maguranye
NextWork Student

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 to flow in and out of the associated subnet. This means every protocol, every port range, and all IP addresses (0.0.0.0/0 for IPv4 and ::/0 for IPv6) are permitted.

In contrast, a custom ACL's inbound and outbound rules are set to deny all traffic by default. Until you define specific allow rules for certain ports, protocols, and IPs, no data can flow in or out of the subnet



The place to learn & showcase your skills

Check out nextwork.org for more projects