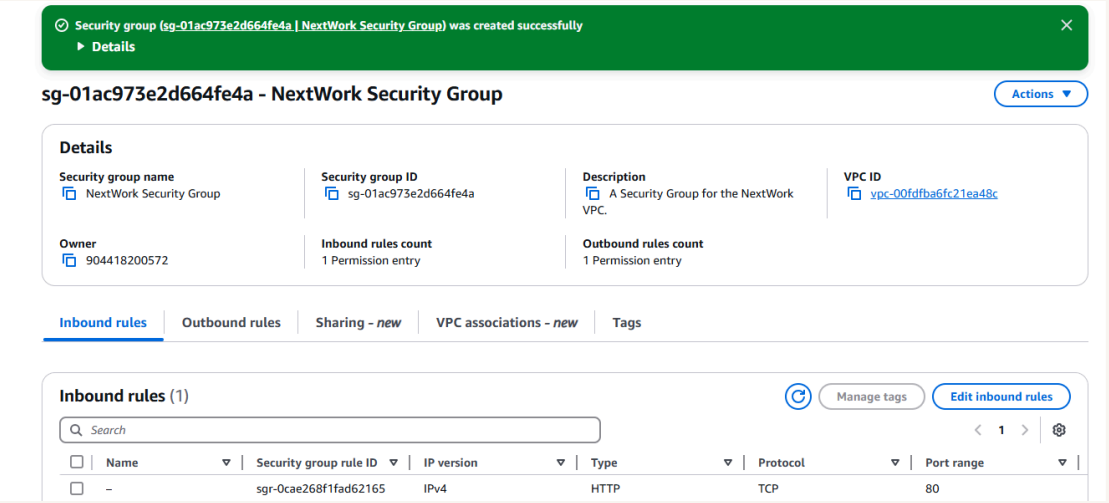
nextwork.org

VPC Traffic Flow and Security

RA **Ranjith D B**



RA
Ranjith D B
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private network in AWS that lets you securely manage resources with custom IP ranges, route tables, and security settings. It’s useful for isolating workloads and controlling traffic flow for better security.

How I used Amazon VPC in this project

I used Amazon VPC to create a secure cloud network with subnets, route tables, a security group, and a network ACL to manage traffic flow and enhance security for resources inside the VPC.

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

I didn’t expect custom network ACLs to block all traffic by default, requiring manual rules for allowing inbound and outbound traffic.

This project took me...

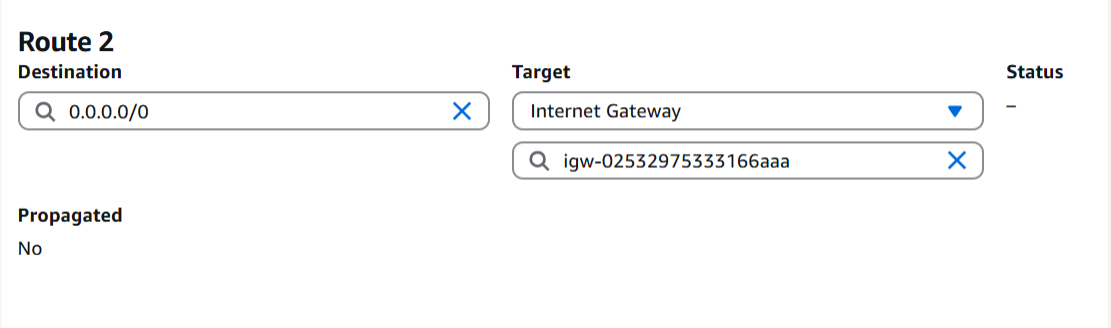
This project took me around one hour to complete, including setting up the VPC, configuring security rules, and associating network ACLs with subnets.

RA
Ranjith D B
NextWork Student

Route tables

Route tables are like a GPS for network traffic, defining rules for where data should go within a VPC. They ensure that resources in a subnet can communicate internally or with external networks.

Route tables are needed to make a subnet public because they define how traffic leaves the VPC. A route directing 0.0.0.0/0 to an internet gateway allows instances to access the internet.

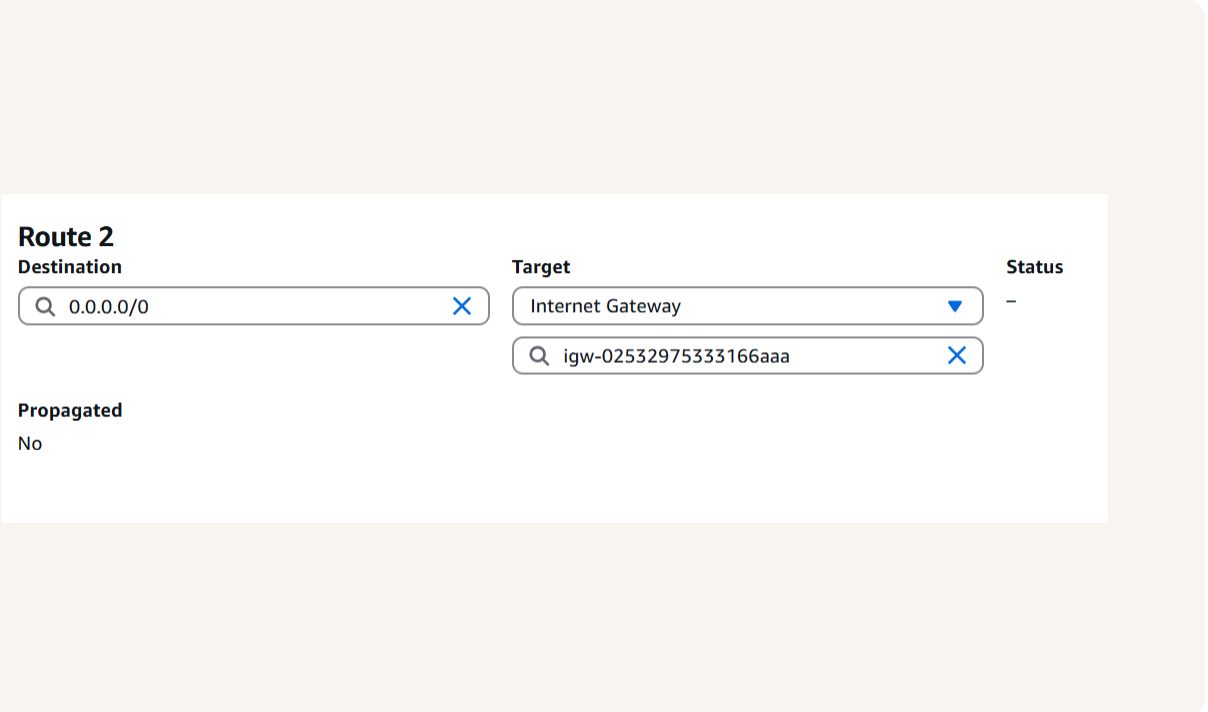


RA
Ranjith D B
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the destination is the IP range traffic wants to reach, while the target is the path it takes (e.g., an internet gateway or local VPC).

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 NextWork IG (Internet Gateway).



RA
Ranjith D B
NextWork Student

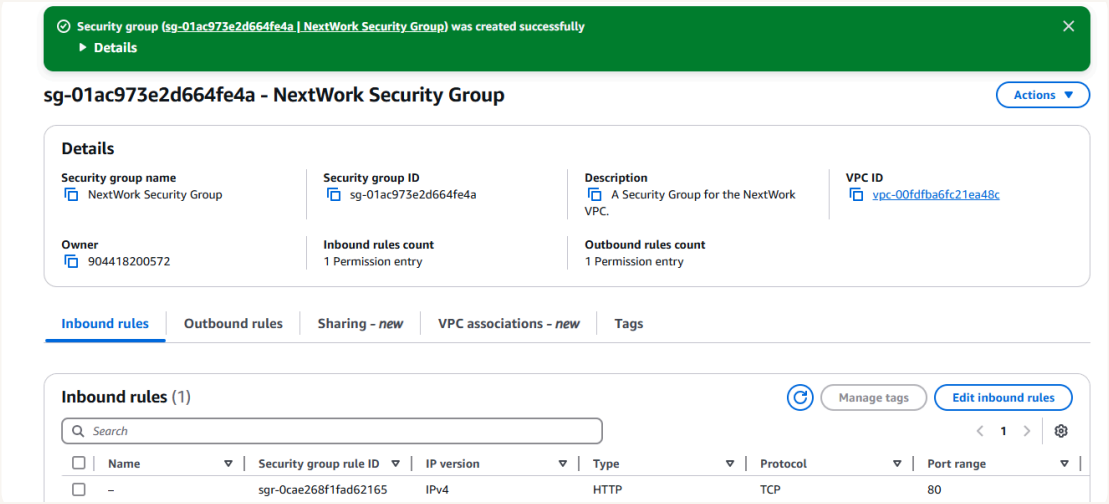
Security groups

Security groups are virtual firewalls that control inbound and outbound traffic to AWS resources. They define who can access a resource and how data flows, ensuring secure communication within a VPC.

Inbound vs Outbound rules

Inbound rules are rules that control traffic entering a resource. I configured an inbound rule that allows HTTP traffic (port 80) from anywhere (0.0.0.0/0), making my resources publicly accessible.

Outbound rules are rules that control traffic leaving a resource. By default, my security group's outbound rule allows all outbound traffic, meaning resources can send data anywhere on the internet.


Security group (sg-01ac973e2d664fe4a | NextWork Security Group) was created successfully
Details
sg-01ac973e2d664fe4a - NextWork Security Group
Actions
Details
Security group name
NextWork Security Group
Security group ID
sg-01ac973e2d664fe4a
Description
A Security Group for the NextWork VPC.
VPC ID
vpc-00fdfba6fc21ea48c
Owner
904418200572
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-0cae268f1fad62165
IPv4
HTTP
TCP
80

RA
Ranjith D B
NextWork Student

Network ACLs

Network ACLs are subnet-level firewalls that control inbound and outbound traffic using stateless rules. They check data packets at the subnet boundary, allowing or denying traffic based on predefined rules.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups apply to individual resources, while network ACLs apply to entire subnets, requiring explicit rules for both inbound and outbound traffic.

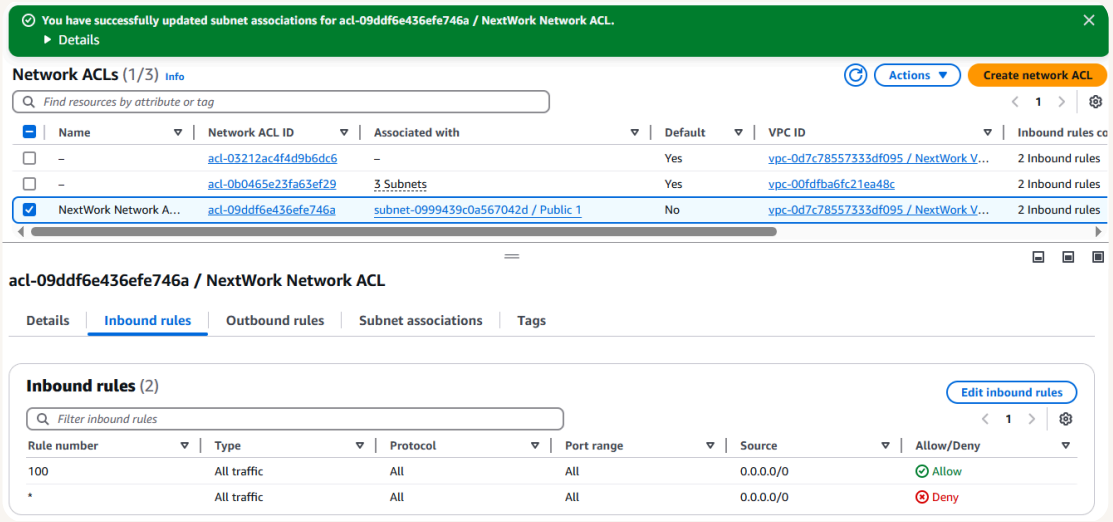
RA
Ranjith D B
NextWork Student

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, meaning any data packet can enter and leave the subnet unless modified by custom rules.

In contrast, a custom ACL’s inbound and outbound rules are automatically set to deny all traffic until specific allow rules are manually added, ensuring no unauthorized access by default.


You have successfully updated subnet associations for acl-09ddf6e436efe746a / NextWork Network ACL.
Details
Network ACLs (1/3) Info
Actions
Create network ACL
Find resources by attribute or tag
Name
Network ACL ID
Associated with
Default
VPC ID
Inbound rules co
– acl-03212ac4f4d9b6dc6 – Yes vpc-0d7c78557333df095 / NextWork V... 2 Inbound rules
– acl-0b0465e23fa63ef29 3 Subnets Yes vpc-00fdfba6fc21ea48c 2 Inbound rules
NextWork Network A... acl-09ddf6e436efe746a subnet-0999439c0a567042d / Public 1 No vpc-0d7c78557333df095 / NextWork V... 2 Inbound rules
acl-09ddf6e436efe746a / NextWork Network ACL
Details
Inbound rules
Outbound rules
Subnet associations
Tags
Inbound rules (2)
Edit inbound rules
Filter inbound rules
Rule number
Type
Protocol
Port range
Source
Allow/Deny
100 All traffic All All 0.0.0.0/0 Allow
* All traffic All All 0.0.0.0/0 Deny

NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects