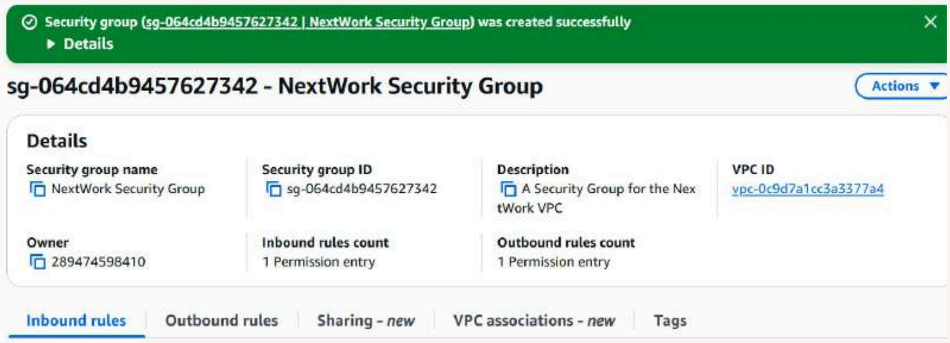
VPC Traffic Flow and Security

GA Mohamed Galole



Security group (sg-064cd4b9457627342 | NextWork Security Group) was created successfully

▸ Details

sg-064cd4b9457627342 - NextWork Security Group

Details

Security group name: NextWork Security Group

Security group ID: sg-064cd4b9457627342

Description: A Security Group for the Nex tWork VPC

VPC ID: vpc-0c9d7a1cc3a3377a4

Owner: 289474598410

Inbound rules count: 1 Permission entry

Outbound rules count: 1 Permission entry

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is virtual network in the AWS cloud that is logically isolated from all other networks. it's useful because It lets you launch AWS resources like EC2 instances or databases, in a customizable, secure network environment that you control.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a secure network with public subnet, internet gateway, and proper route table and security groups for controlled app access and isolation.

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

One thing I didn't expect in this project was, I didn’t expect how crucial proper route table and subnet configuration would be a small mistake caused connectivity issues between instances in public and private subnets.

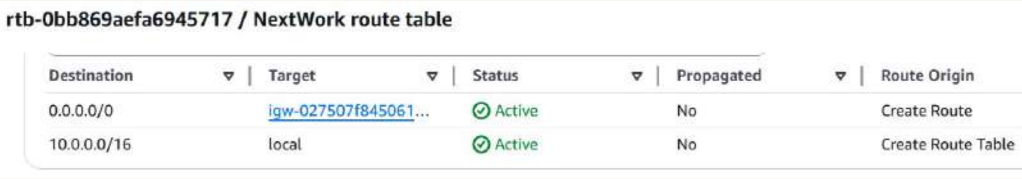
This project took me...

This project took me one hour twenty minutes

Route tables

Route tables are set of rules that determine where network traffic should go inside your VPC (Virtual Private Cloud).

Routes tables are needed to make a subnet public because a subnet becomes public when its route table has a route to an Internet Gateway that’s what gives it access to and from the Internet.



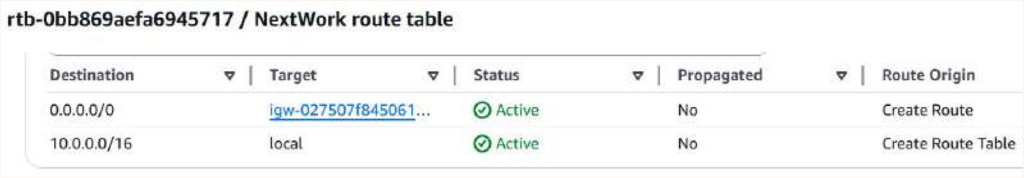
rtb-0bb869aefa6945717 / NextWork route table

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-027507f845061...	✓ Active	No	Create Route
10.0.0.0/16	local	✓ Active	No	Create Route Table

Route destination and target

Routes are defined by their destination and target, which mean Destination is where the traffic is going and Target is how it will get there.

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.



rtb-0bb869aefa6945717 / NextWork route table

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-027507f845061...	✓ Active	No	Create Route
10.0.0.0/16	local	✓ Active	No	Create Route Table

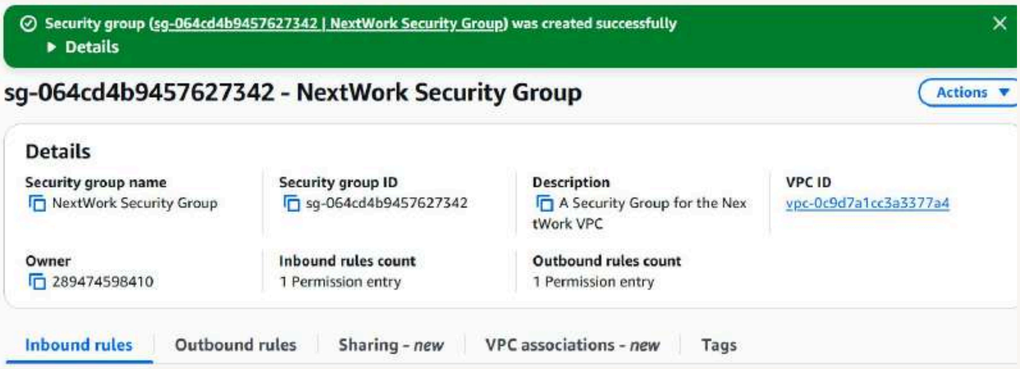
Security groups

Security groups act as virtual firewalls that controls inbound and outbound traffic for your EC2 instances and other resources (like RDS databases or Lambda functions in a VPC).

Inbound vs Outbound rules

Inbound rules defines what kind of incoming traffic is allowed to reach your AWS resource I configured an inbound rule that allow web traffic from anywhere.

Outbound rules defines what kind of outgoing traffic is allowed from your AWS resource to other destinations such as the Internet, another VPC, by default, my security group's outbound rule allow all outbound traffic to all destinations.



Security group (sg-064cd4b9457627342 | NextWork Security Group) was created successfully

▸ Details

sg-064cd4b9457627342 - NextWork Security Group

Details

Security group name: NextWork Security Group

Security group ID: sg-064cd4b9457627342

Description: A Security Group for the NextWork VPC

VPC ID: vpc-0c9d7a1cc3a3377a4

Owner: 289474598410

Inbound rules count: 1 Permission entry

Outbound rules count: 1 Permission entry

Network ACLs

Network ACLs are virtual firewalls that controls inbound and outbound traffic at the subnet level in your AWS VPC. It acts as the first line of defense deciding what kind of traffic is allowed into or out of a subnet before it reaches your EC2.

Security groups vs. network ACLs

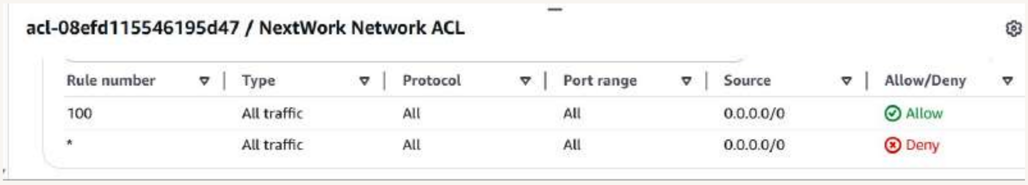
The difference between a security group and a network ACL is that ACLs control traffic at the subnet level while Security Groups control traffic at the instance level.

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 inbound and outbound traffic.

In contrast, a custom ACL’s inbound and outbound rules are automatically set to denied. By default, no inbound/outbound rules exist. Therefore: All inbound/outbound traffic is denied by default.



acl-08efd115546195d47 / NextWork Network ACL

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

The place to learn & showcase your skills

Check out nextwork.org for more projects