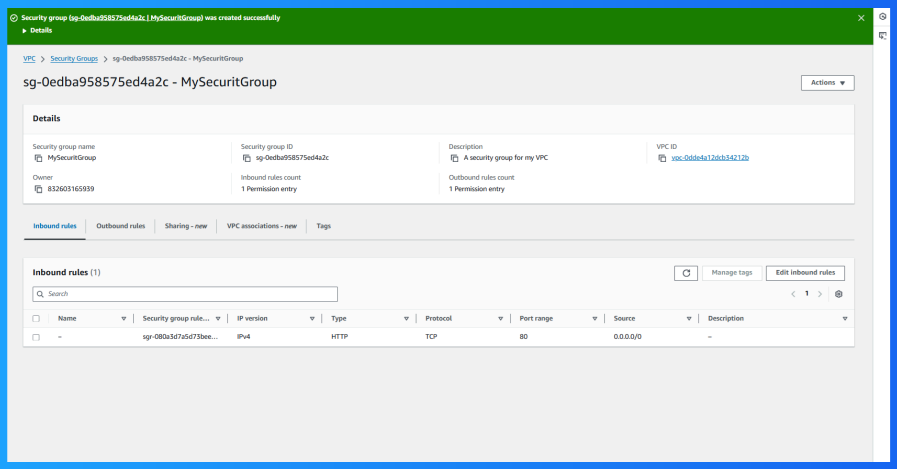
NextWork.org

VPC Traffic Flow and Security

RAJARSHI VERMA



R
RAJARSHI VERMA
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows you to create a private, isolated network within the AWS cloud. It provides security, customization, and scalability, enabling you to control inbound and outbound traffic, connect to the internet, and manage.

How I used Amazon VPC in this project

I created a VPC with subnet and internet gateway. Then further I created a route table and then created a security group and at last created a network ACL.

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

Already created security groups and default rules and ACl. Moreover it is easy to create and set our rules but understanding of address and ports is necessary.

This project took me...

It took me not more than 15 minutes for all the progress.

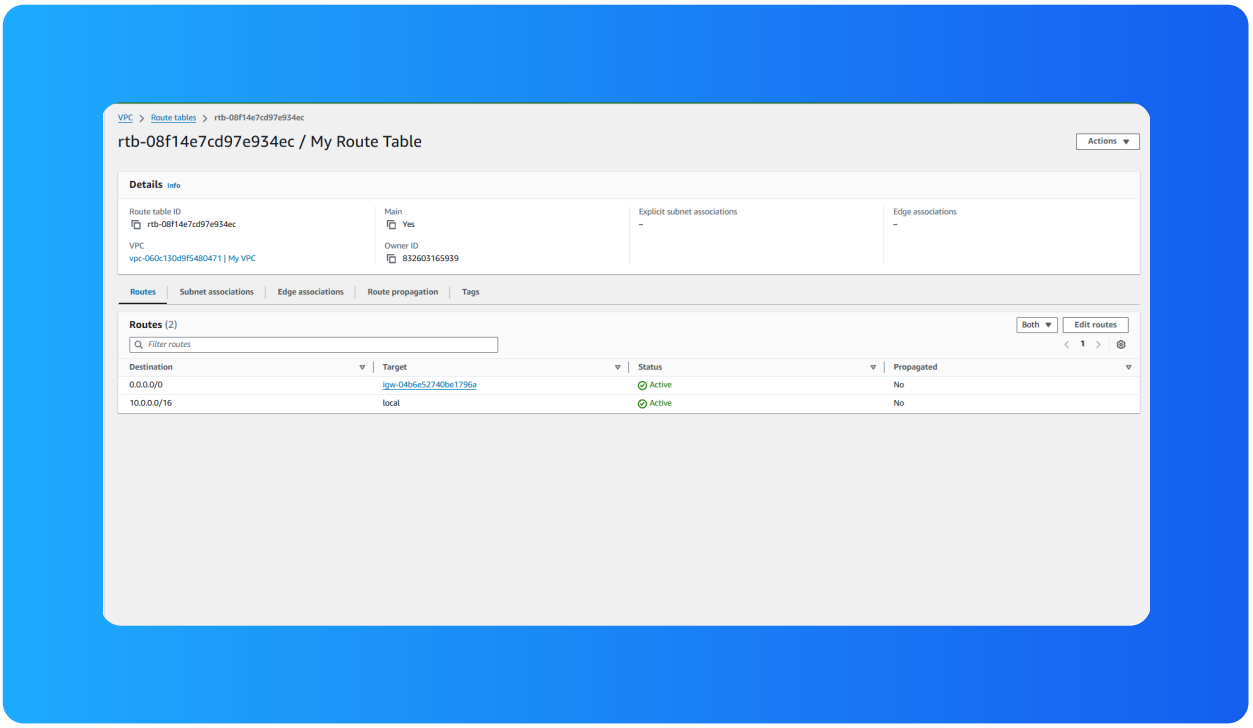
R

RAJARSHI VERMA
NextWork Student

Route tables

A route table in a VPC acts like a GPS, guiding data to its destination. Each subnet needs a route table to direct traffic. Without it, resources can't send or receive data. Multiple subnets can share one route table, but each subnet can only use one

Route tables are needed to make a subnet public because they direct traffic to the internet gateway. Without a route table, the subnet wouldn't know where to send or receive data, making it impossible for resources to communicate with the internet.

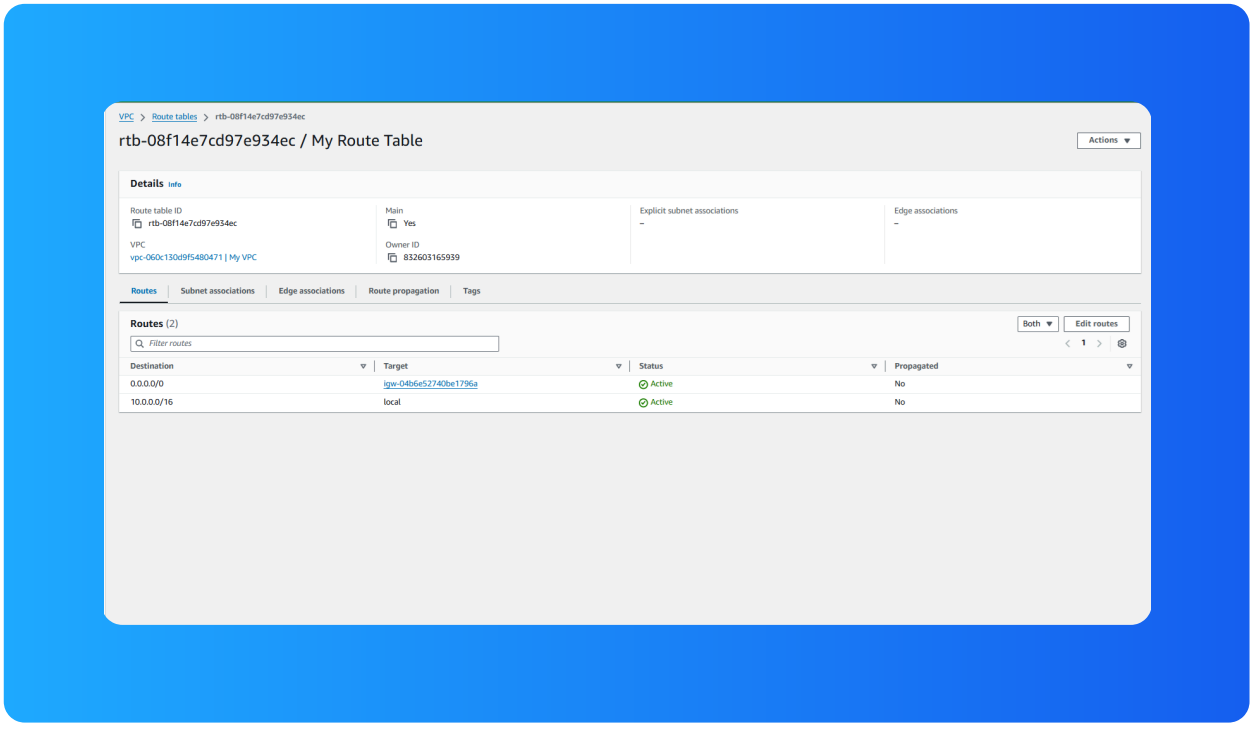


R
RAJARSHI VERMA
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the IP address range that traffic wants to reach and the path it takes to get there. Example, `0.0.0.0/0` as a destination means all IP addresses, and `igw-xxxx` as target means IG.

New routes destination is 10.0.0.0/16 and target as local and if not found we have added a 0.0.0.0/0 destination whose target is internet gateway and it will search on web.



R

RAJARSHI VERMA
NextWork Student

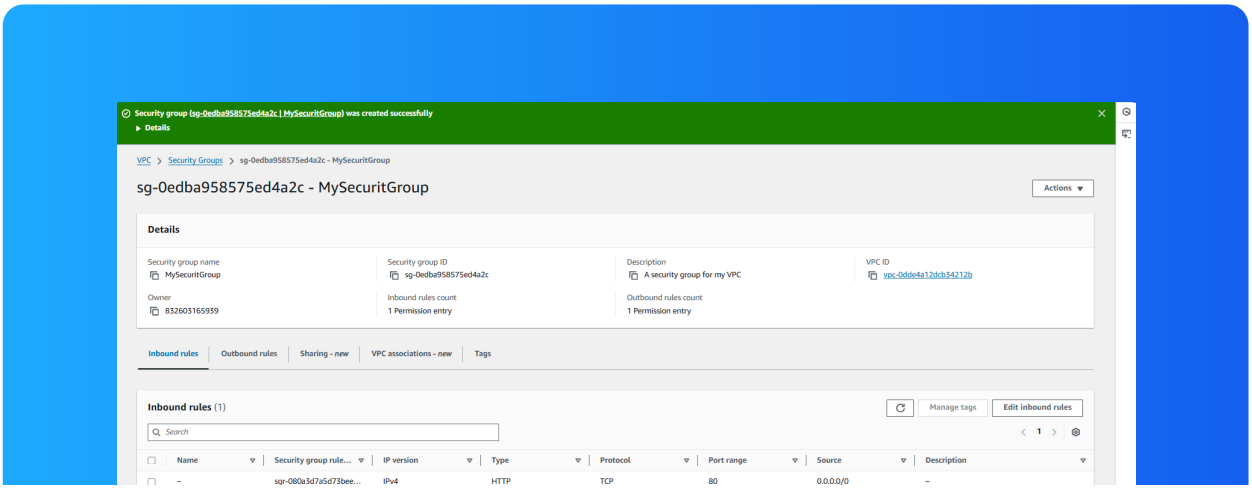
Security groups

Security groups are virtual firewalls for your AWS resources. They control inbound and outbound traffic to and from your resources based on rules you define. Each security group acts at the instance level and allows which traffic to interact.

Inbound vs Outbound rules

Inbound rules are rules that control the incoming traffic to your resources. They specify which traffic is allowed to enter your resources based on criteria like IP address, protocol, and port number. I added type HTTP and Source type anywhere IPv-4.

Outbound rules are rules that control the outgoing traffic from your resources. By default, my security group's outbound rule allows all outbound traffic, meaning any resource associated with the security group can send data to any IP address.



R
RAJARSHI VERMA
NextWork Student

Network ACLs

A Network Access Control List (ACL) are set of rules that control network traffic in and out of a subnet.. Imagine a traffic cop standing at the entrance and exit of your subnet. Each time a data packet tries to enter or leave, the traffic cop check

Security groups vs. network ACLs

The difference between a security group and a network ACL is that ACL is a firewall that controls traffic for an entire subnet. And Security groups are more granular than ACLs. They control traffic for individual resources, such as EC2 instance.

R

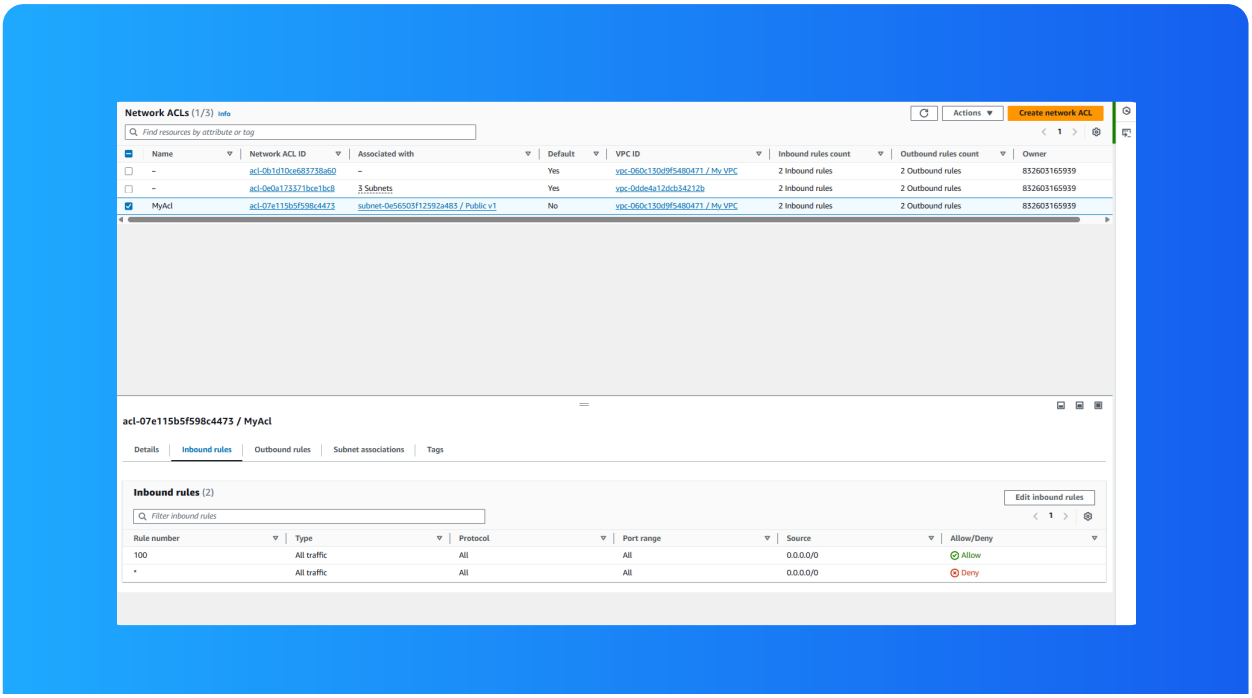
RAJARSHI VERMA
NextWork Student

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. This means that all incoming and outgoing traffic is permitted unless you specifically add rules to deny certain types of traffic or restrict access to specific IP address

In contrast, a custom ACL’s inbound and outbound rules are automatically set to **deny all traffic**. This means that no data can enter or leave the associated subnets until specific rules are added. By default, all traffic is blocked.



Everyone should be in a job they love.

Check out nextwork.org for more projects