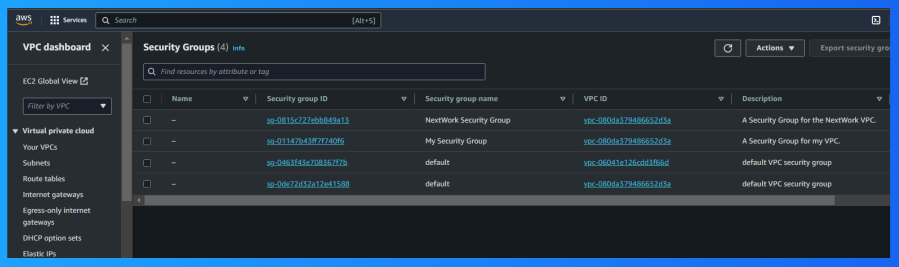
NextWork.org

VPC Traffic Flow and Security

sirajudeen athif



S
sirajudeen athif
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that allows users to create private networks within the AWS cloud. It provides enhanced security, customizable network configurations and easy scalability.

How I used Amazon VPC in this project

I used Amazon VPC to create a private network, which I then connected to a route table and network ACL for internet access and security.

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

Using AWS services is quite straightforward; it just requires some practice.

This project took me...

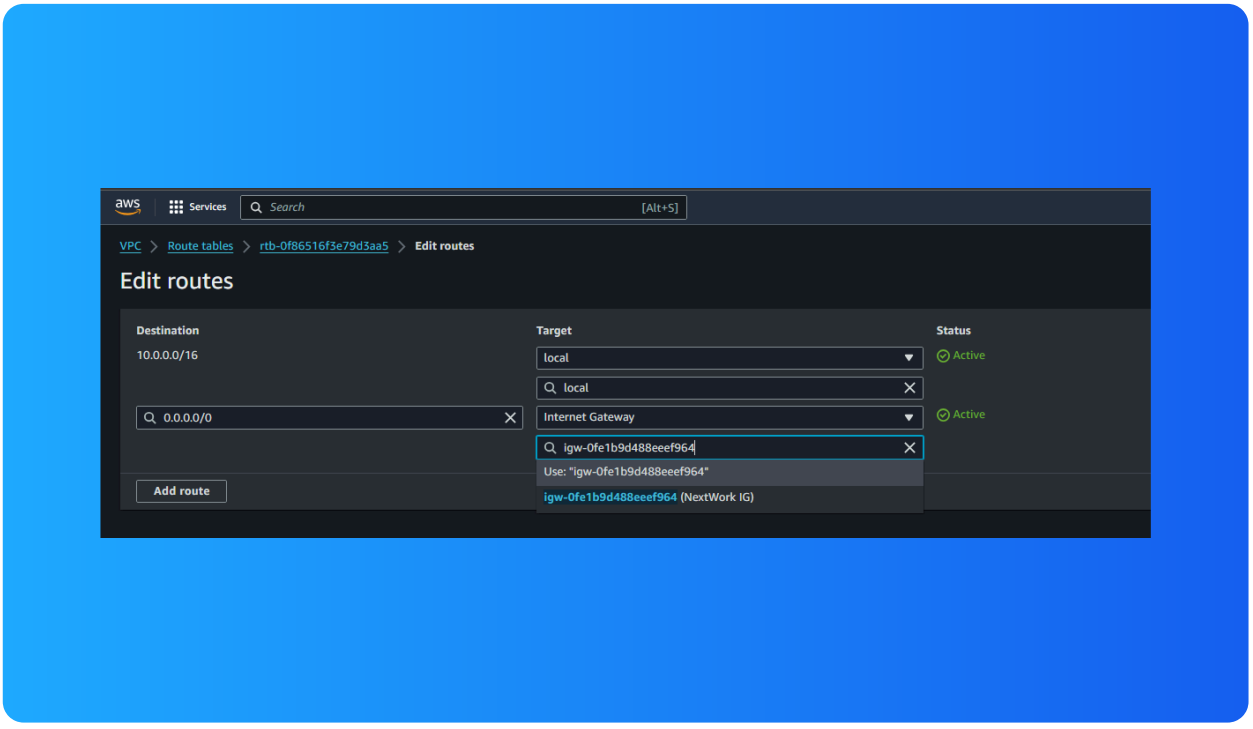
I completed the implementation almost immediately, while the documentation took about an hour.

S
sirajudeen athif
NextWork Student

Route tables

Route tables are a table of rules, called Routes, that decide where the data in the network should go. They function as a GPS for the resources in the subnet; Without them, the resources would lack direction of sending or receiving data.

Routes tables are needed to make a subnet public because they contain rules that direct the traffic from the network to the internet gateway, which in turn allows the resources within the subnet to have access to the internet.

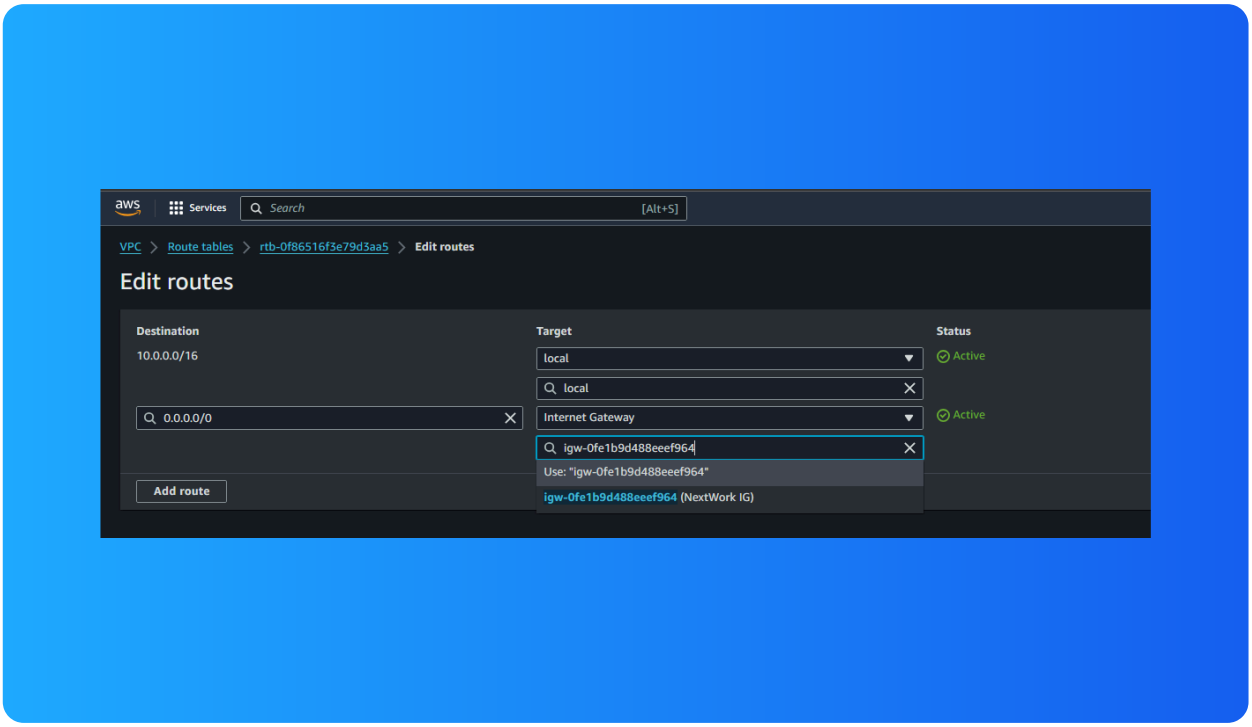


S
sirajudeen athif
NextWork Student

Route destination and target

Destination: It refers to the IP address that network traffic intends to reach.
Target: The path that the traffic will have to take 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-0fe1b9d488eeef964, which is the internet gateway ID.



sirajudeen athif
NextWork Student

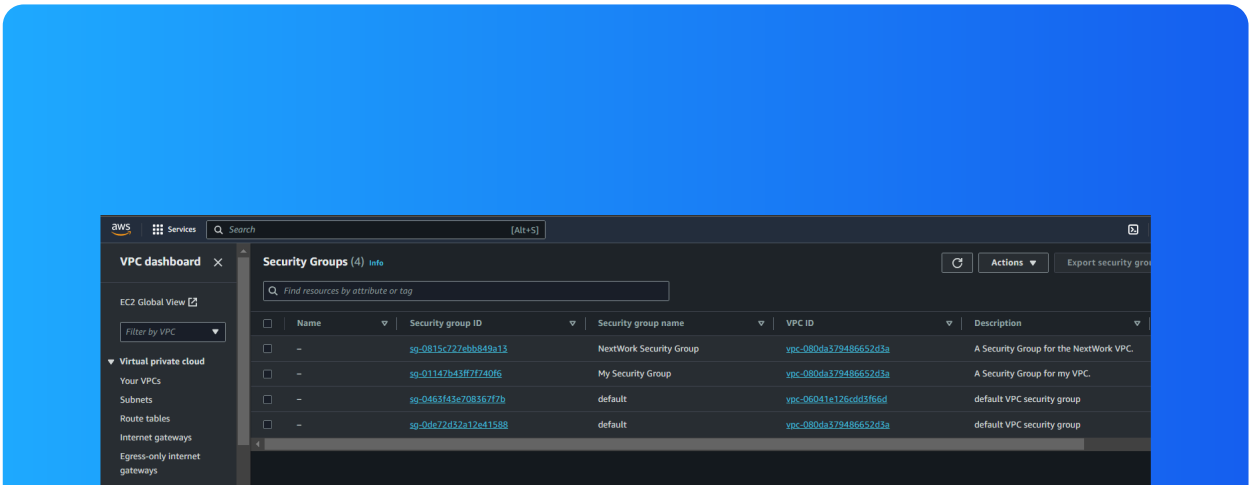
Security groups

Security groups act as security checkpoints for the resources within your subnet. They must be associated with the resources, not the VPC or the subnet. They enforce rules upon incoming and outgoing data based on IP addresses, protocols, etc.

Inbound vs Outbound rules

Inbound rules are applied to data entering your resource within a security group. I configured an inbound rule of type HTTP, meaning it allows incoming traffic on port 80, allowing the web traffic to reach the resource to serve HTTP requests.

Outbound rules are rules that are enforced on data that is being sent out. By default, my security group's outbound rule allows all outgoing traffic, meaning any resource associated with this security group can send data without any restrictions.



S
sirajudeen athif
NextWork Student

Network ACLs

Network ACLs (Access Control Lists) act as an optional security layer for controlling inbound and outgoing traffic. A subnet can only be associated with one network ACL at a time.

Security groups vs. network ACLs

The difference between a security group and a network ACL lies in their level of control. Network ACLs apply broad traffic rules to an entire subnet, while security groups provide more granular control, allowing specific rules for individual resource

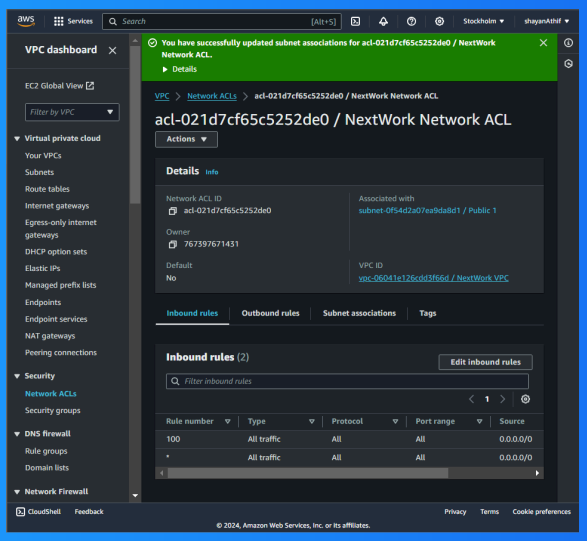
sirajudeen athif
NextWork Student

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 be to allow all inbound and outgoing traffic within the network, unless customized.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all inbound and outgoing traffic, meaning they do not allow any data to enter or exit. You must explicitly add rules to allow specific types of data.



Everyone should be in a job they love.

Check out nextwork.org for more projects