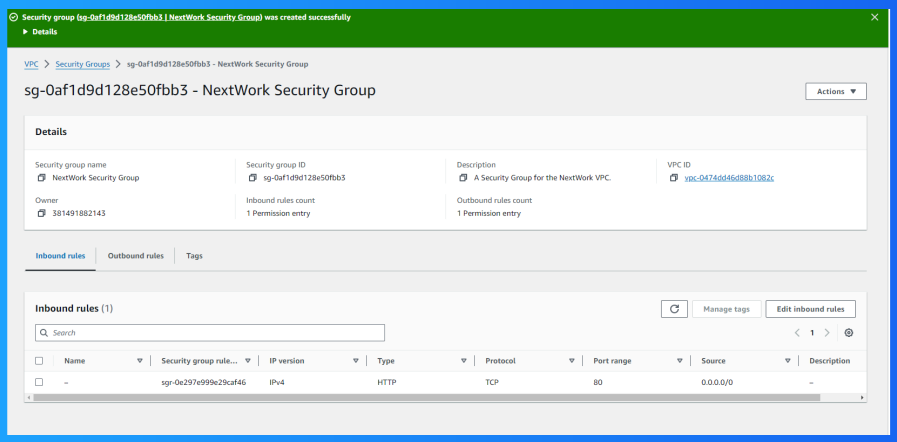
NextWork.org

VPC Traffic Flow and Security

Sai Prasanth Reddy



Sai Prasanth Reddy
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that lets you create isolated cloud networks in AWS. It’s useful because it provides control over networking, including IP ranges, subnets, and security, enabling secure, scalable, and customizable cloud infrastructure.

How I used Amazon VPC in this project

I used Amazon VPC in today's project to create an isolated network, set up subnets, attached an internet gateway, and configured route tables and security groups to ensure proper network access and security for my resources.

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

One thing I didn't expect in this project was the complexity of configuring network settings, especially ensuring the correct routing and security group rules for internet access through the public subnet.

This project took me...

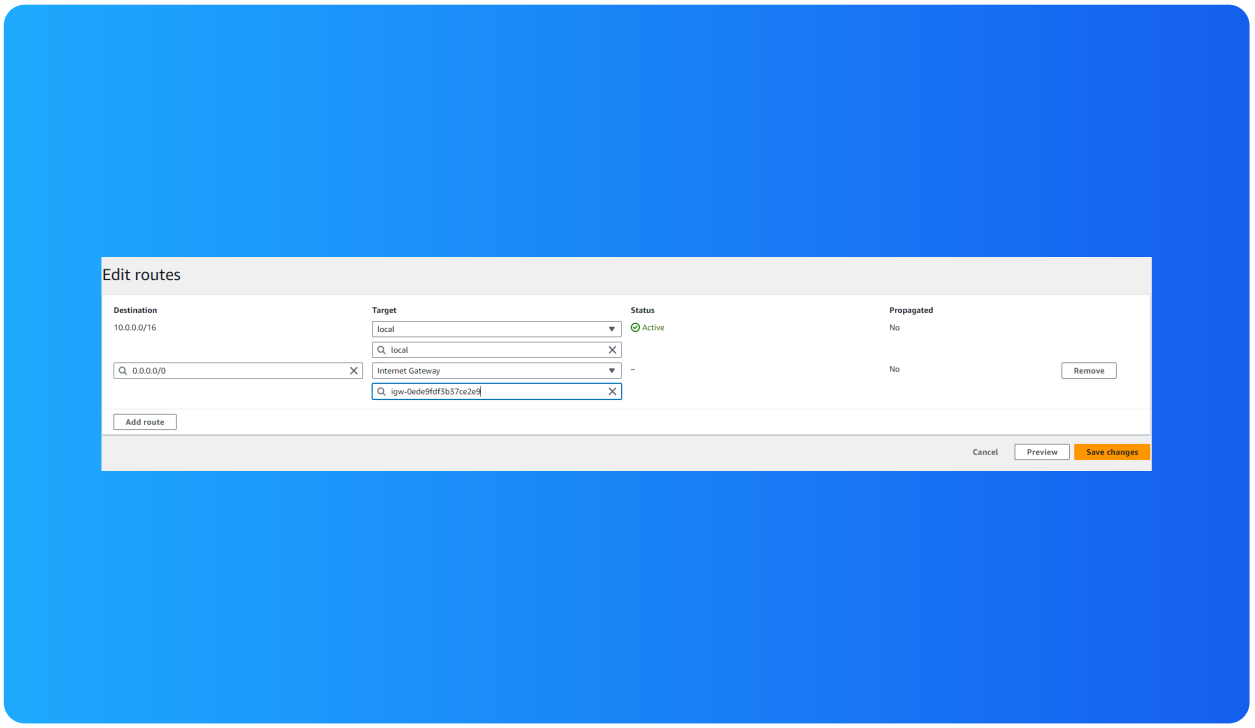
This project took me about an hour, mainly due to configuring the VPC, subnets, internet gateway, and adjusting the route tables and security settings.

Sai Prasanth Reddy
NextWork Student

Route tables

Route tables are sets of rules within a VPC that determine how traffic is directed between subnets and external networks. They specify the destination IP ranges and the target (like an internet gateway or NAT) for routing traffic.

Route tables are needed to make a subnet public because they define the path for outbound traffic to the internet. A public subnet requires a route that directs traffic to the internet gateway, allowing instances to communicate externally.

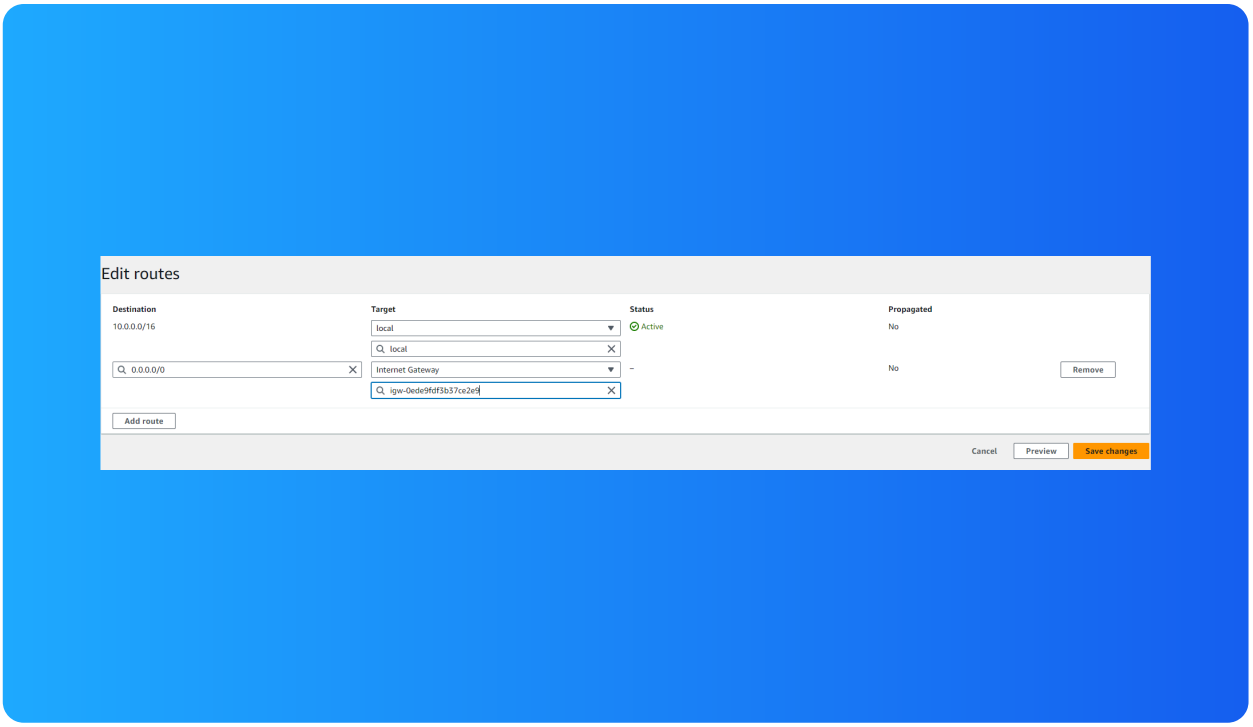


Sai Prasanth Reddy
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the destination specifies the IP range for the traffic, and the target indicates where that traffic should be sent, such as an internet gateway, NAT gateway, or another subnet.

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of 0.0.0.0/0, meaning all traffic, and a target of the internet gateway, allowing external communication.



Sai Prasanth Reddy
NextWork Student

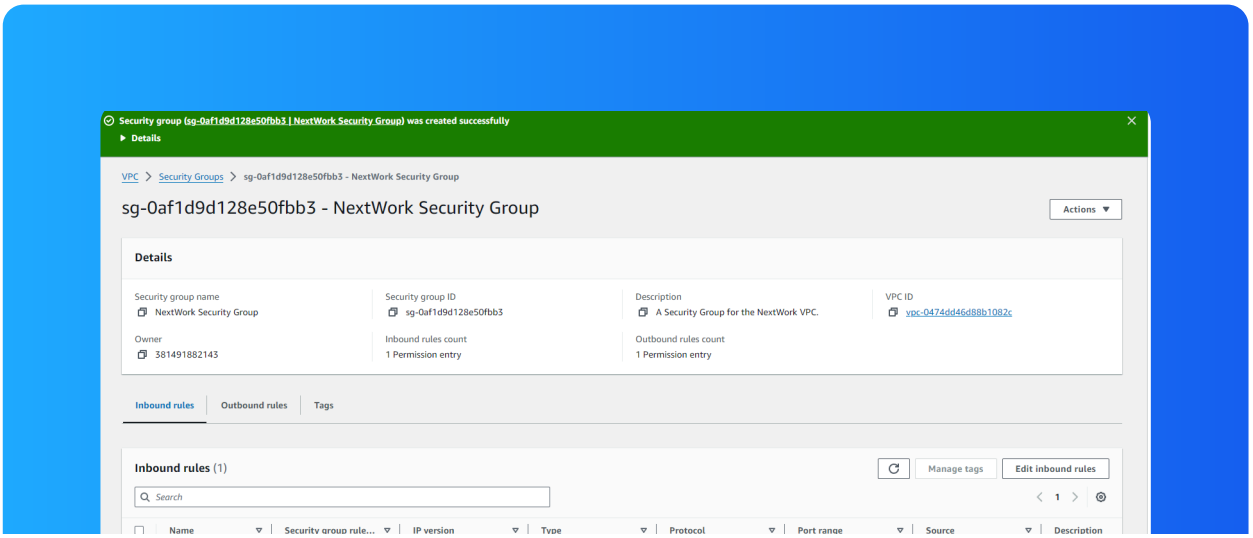
Security groups

Security groups are virtual firewalls that control inbound and outbound traffic for AWS resources. They allow you to define rules based on IP addresses, protocols, and ports, ensuring only authorized traffic reaches or leaves your instances.

Inbound vs Outbound rules

Inbound rules are rules that define the type of incoming traffic allowed to reach a resource. I configured an inbound rule that allows HTTP traffic (port 80) from any IP address, enabling web access to my instances.

Outbound rules are rules that define the type of outgoing traffic allowed from a resource. By default, my security group's outbound rule allows all outbound traffic to any destination, ensuring that my instances can communicate with external networks



Sai Prasanth Reddy
NextWork Student

Network ACLs

Network ACLs are stateless firewalls at the subnet level that control both inbound and outbound traffic. They allow you to set rules for allowing or denying traffic based on IP addresses, protocols and ports, applying to all resources within a subnet

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are stateful, meaning return traffic is automatically allowed, while network ACLs are stateless, requiring explicit rules for both inbound and outbound traffic.

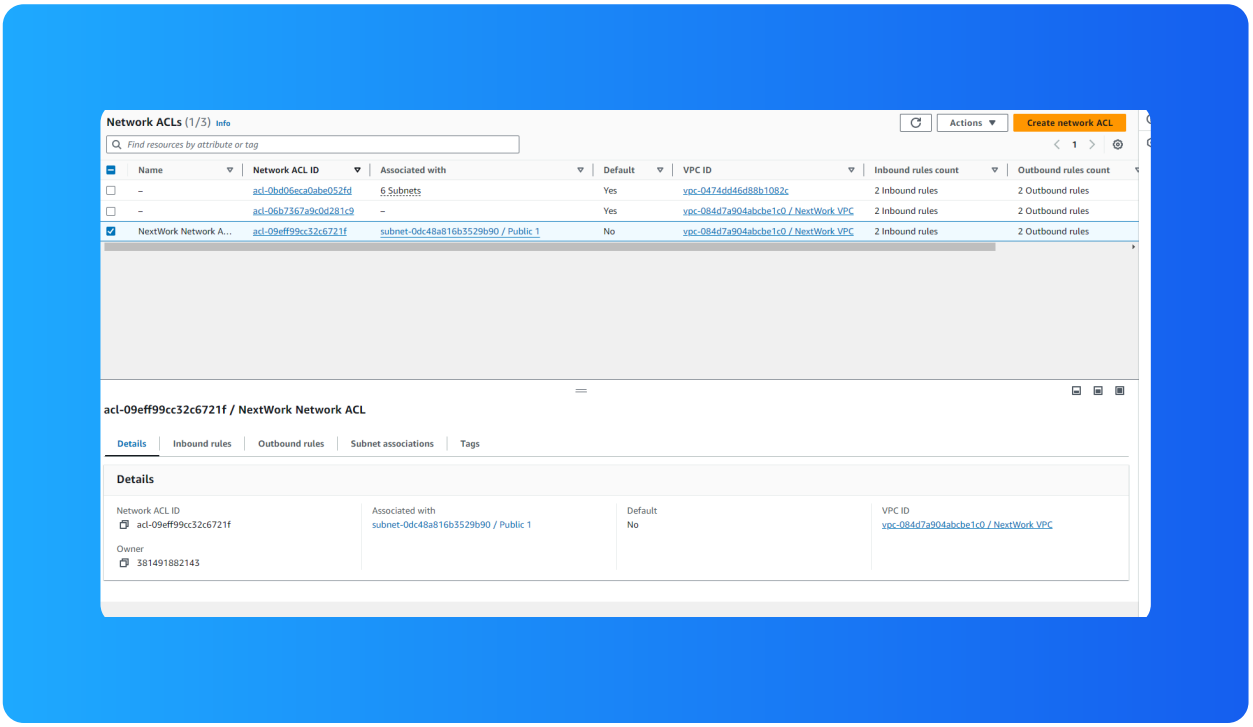
Sai Prasanth Reddy
NextWork Student

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 both inbound and outbound traffic is permitted unless specific deny rules are added.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic by default, requiring you to manually configure specific rules to allow desired traffic through the network.



Everyone should be in a job they love.

Check out nextwork.org for more projects