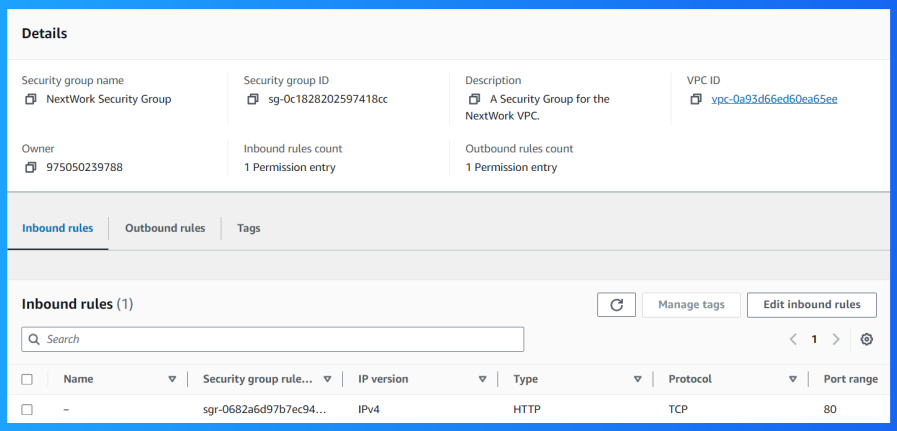
NextWork.org

VPC Traffic Flow and Security

SH shravanirg03@gmail.com



SH
shravanirg03@gmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC allows you to create an isolated, secure network in the AWS cloud, giving you control over IP ranges, subnets, etc. It is useful as it enhances security, and lets you scale resources while ensuring privacy and flexibility.

How I used Amazon VPC in this project

To ensure optimal traffic flow and security, I created a subnet within an Amazon VPC and configured routing tables, security groups, and network ACLs.

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

This project provided valuable insights and deeper understanding of various networking concepts.

This project took me...

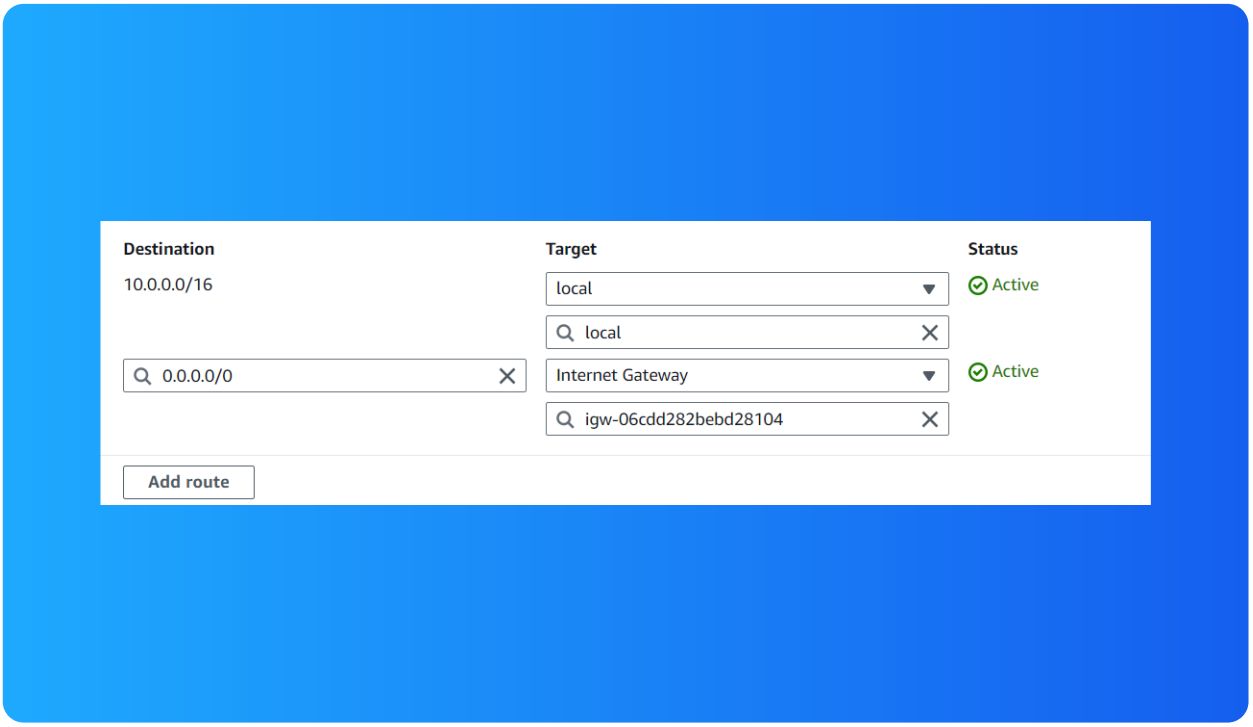
The entire process took me approximately 60 minutes.

SH
shravanirg03@gmail.com
NextWork Student

Route tables

Route tables in AWS define how network traffic is directed within a VPC. They contain a set of rules, or routes, that specify where to send network traffic based on its destination IP address.

Routes tables are needed to make a subnet public because they have a route pointing to an Internet Gateway for all outbound traffic. This route allows resources in the subnet to communicate with the internet, making it publicly accessible.

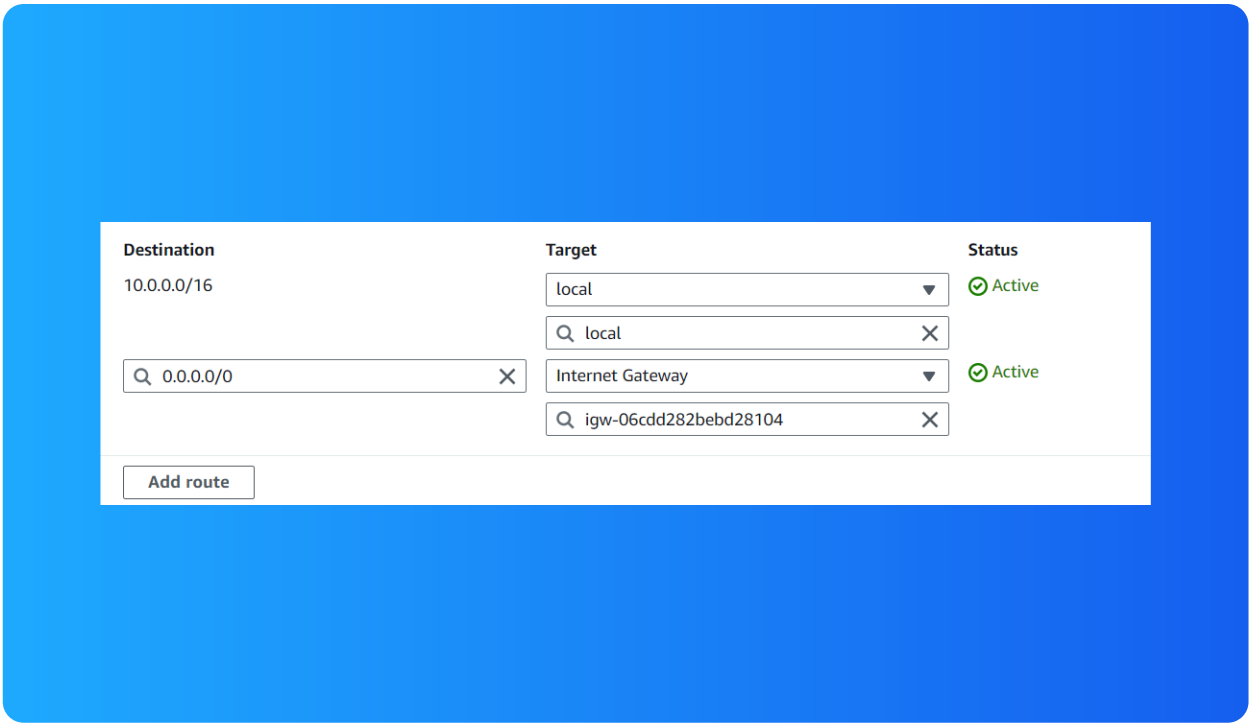


SH
shravanirg03@gmail.com
NextWork Student

Route destination and target

Routes are defined by their destination and target, where the destination is the range of IP addresses the traffic in my VPC is trying to reach and the target is the road/path that the traffic will use to get to their 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 my NextWork IG (internet gateway).



SH
shravanirg03@gmail.com
NextWork Student

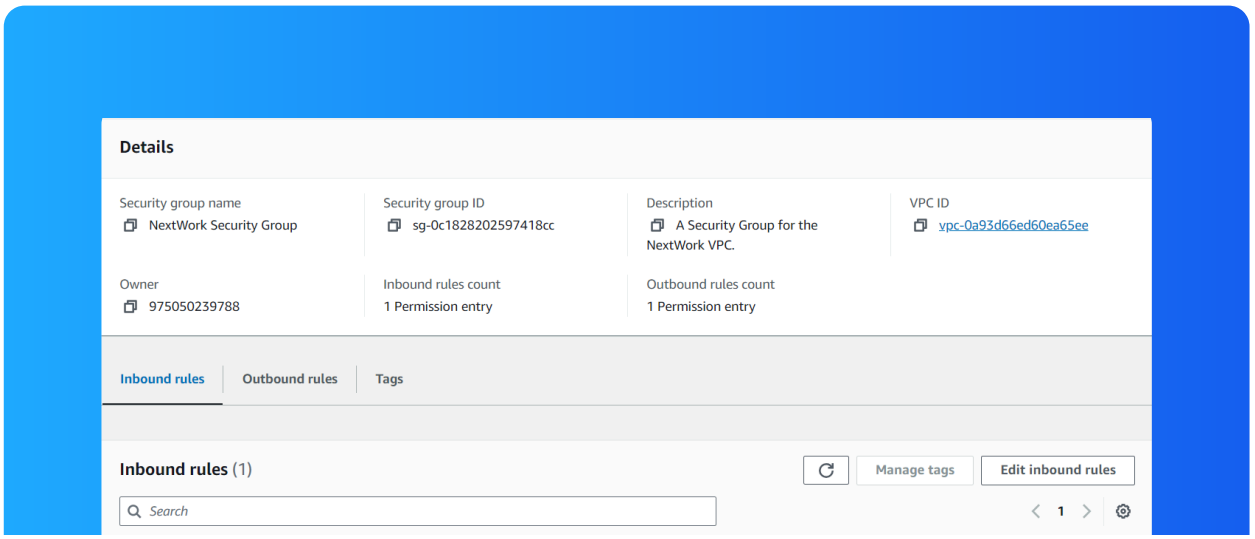
Security groups

Security groups are used for controlling inbound and outbound traffic to resources like EC2 instances. They define the allowed traffic based on protocols, ports, and IP ranges. Every single resource in a subnet/VPC has a security group.

Inbound vs Outbound rules

Inbound rules are the rules that specifies which traffic from outside the security group can enter instances. E.g. Users visiting a web app I'm hosting. I configured an inbound rule that allows all HTTP inbound traffic.

Outbound rules are the rules that specifies which traffic from instances can leave the security group. E.g. My web app requesting data from a public source. By default, my security group's outbound rule will allow all outbound traffic.



SH
shravanirg03@gmail.com
NextWork Student
NextWork.org

Network ACLs

Network ACLs are control traffic at the subnet level in AWS. They allow or deny traffic based on IP addresses, protocols, and ports for both inbound and outbound traffic.

Security groups vs. network ACLs

The difference between a security group and a network ACL is their scope i.e. a security group secures my network at the resource level, while network ACLs secure my network at the subnet level.

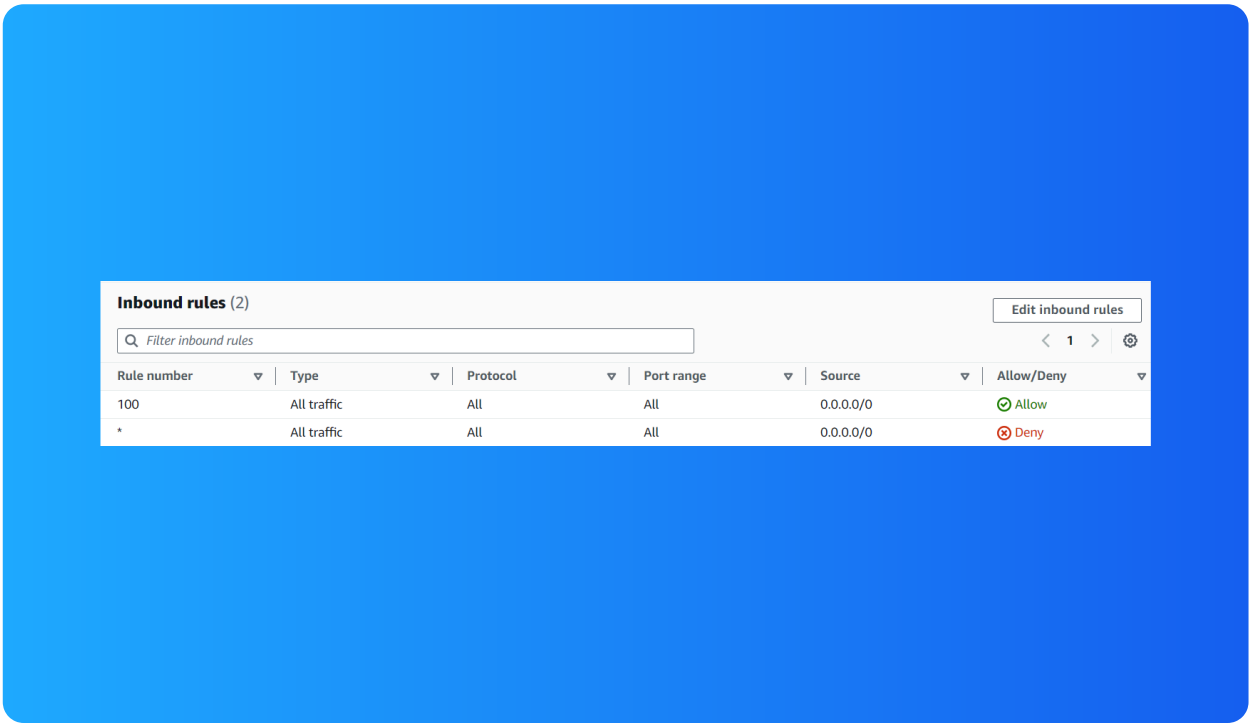
SH
shravanirg03@gmail.com
NextWork Student

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 rule is set up to allow all incoming and outgoing traffic, respectively. This means that no restrictions are applied unless explicitly modified.

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



Everyone should be in a job they love.

Check out nextwork.org for more projects