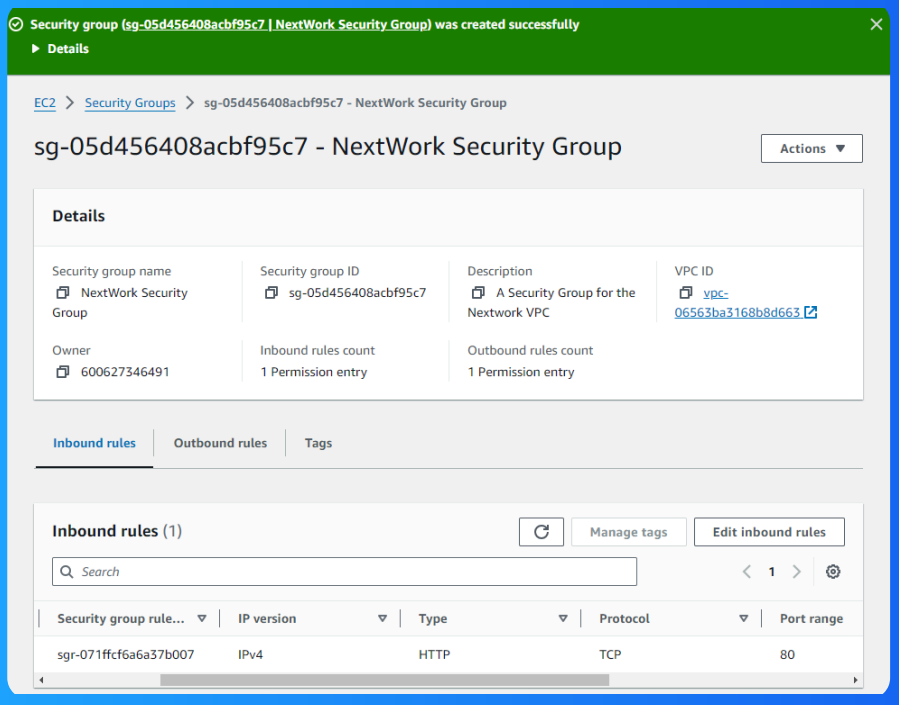
NextWork.org

VPC Traffic Flow and Security

Ivan Delgadillo Fernandez



Ivan Delgadillo Fernandez
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud (Amazon VPC) gives you full control over your virtual networking environment, including resource placement, connectivity, and security

How I used Amazon VPC in this project

I created VPC to put a subnet facing to internet

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

I didn't expect to configure the network ACL

This project took me...

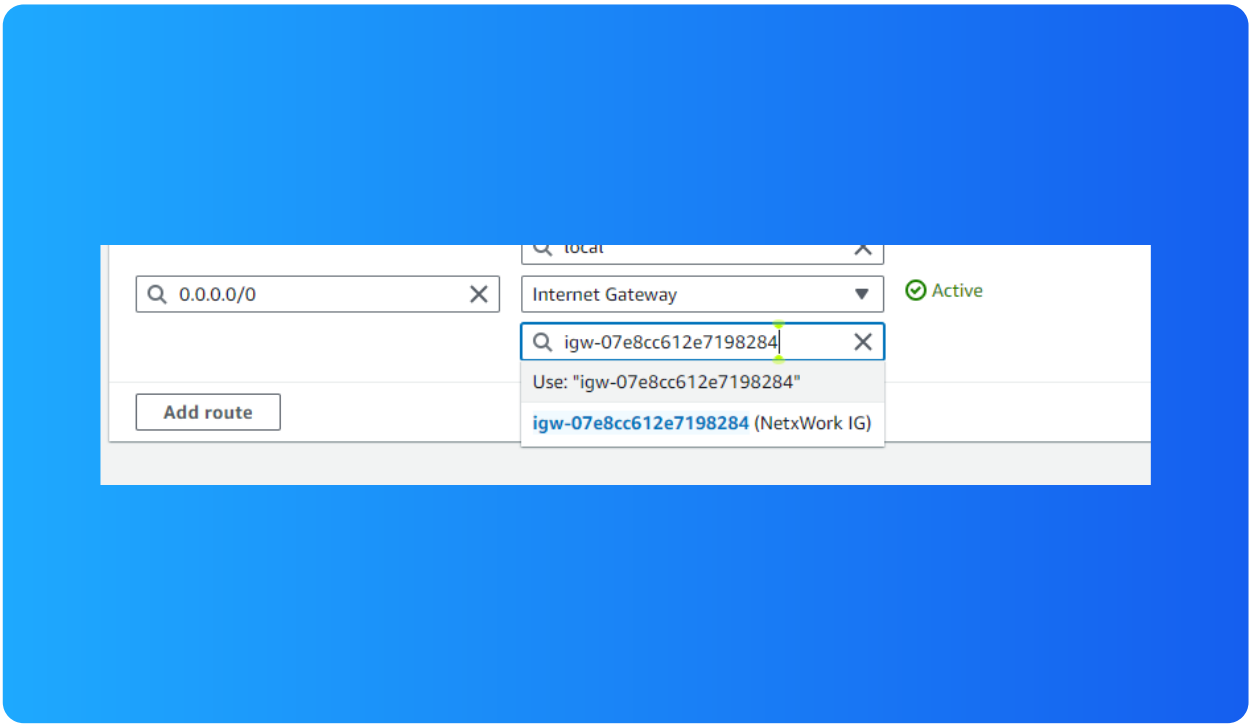
around 45 minutes

Ivan Delgadillo Fernandez
NextWork Student

Route tables

Route table are a set of rules, known as routes that determines where network traffic is directed.

Route tables are needed to make a subnet public for Internet access.

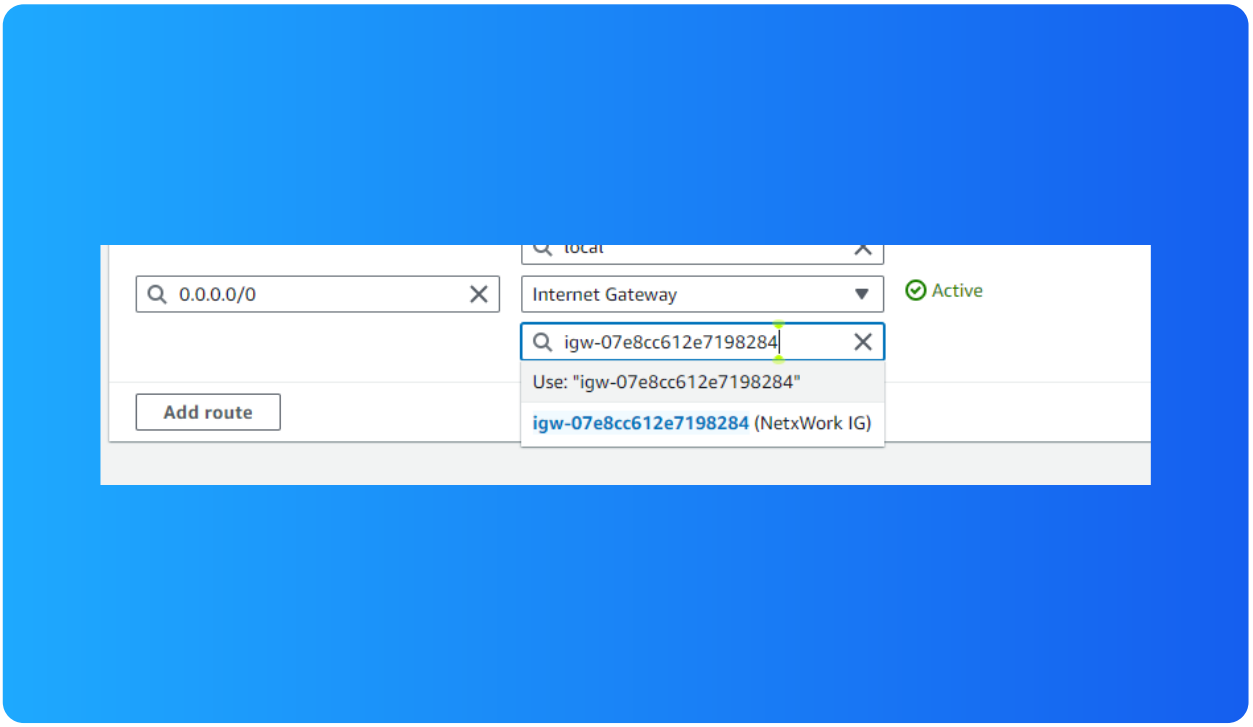


Ivan Delgadillo Fernandez
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean network traffic can be redirected

The route in my route table that directed internet-bound traffic to my internet gateway had destination of anywhere, and a target of my internet gateway.



Ivan Delgadillo Fernandez
NextWork Student

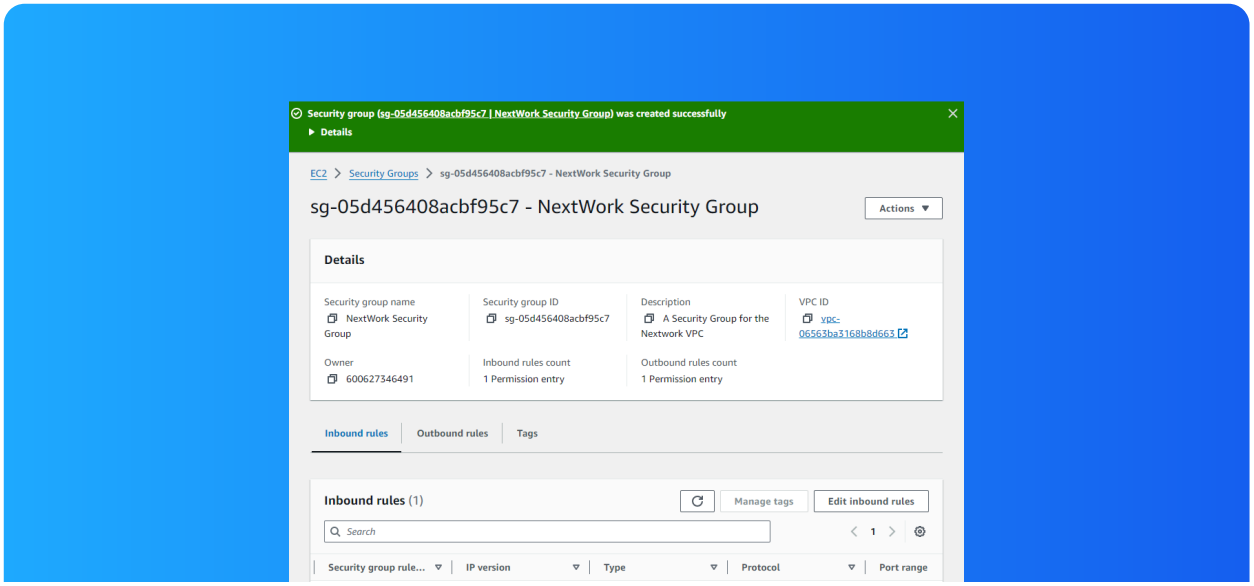
Security groups

Security groups are responsible for checking who comes in and out. They have strict rules about what kind of traffic can enter or leave the resource based on its IP address, protocols and port numbers.

Inbound vs Outbound rules

Inbound rules control the data that can enter the resources in your security group, while outbound rules control that data that your resources can send out.

By default, AWS security groups already allow all outbound traffic. So unless you specify otherwise, any resource associated with the security group can access and send data to any IP address - whether it's in your VPC, other VPCs (if you have the ri



Ivan Delgadillo Fernandez
NextWork Student

Network ACLs

Network ACL are a rules that either allow access to a network.

Security groups vs. network ACLs

Security groups and network ACLs are similar in that they allow you to control access to AWS resources within your VPC. But security groups allow you to control inbound and outbound traffic at the instance level, while network ACLs offer similar capa

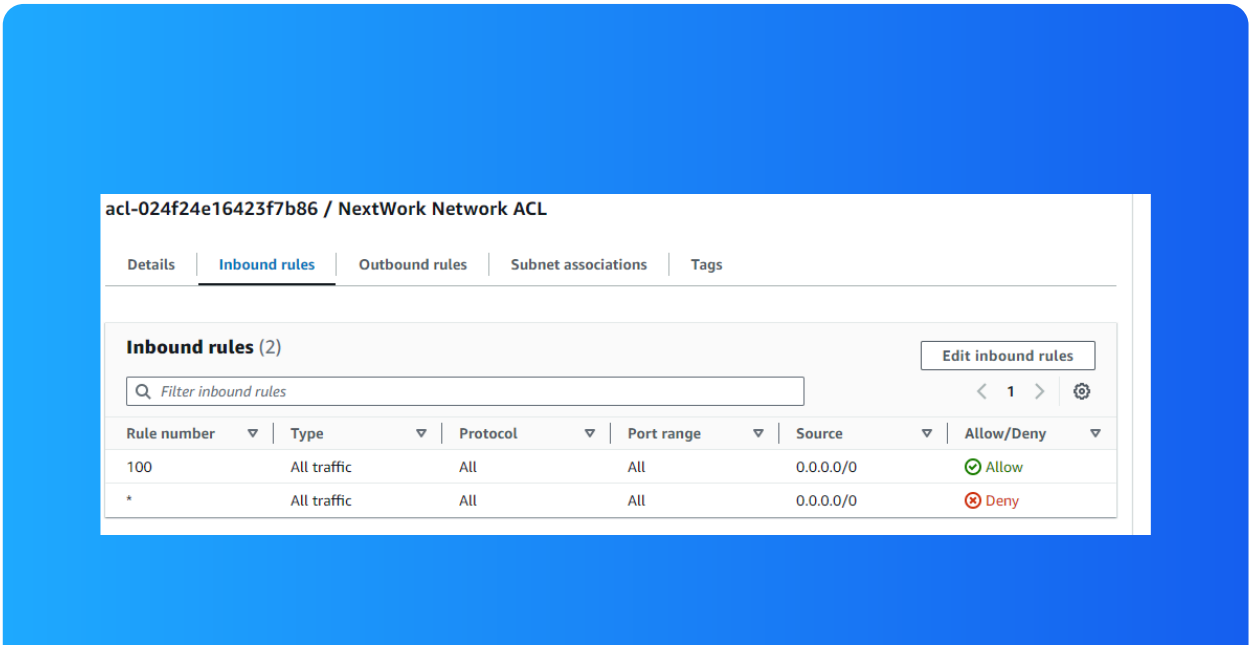
Ivan Delgadillo Fernandez
NextWork Student

Default vs Custom Network ACLs

Similar to security groups, network ACLs use inbound and outbound rules

The default network ACL is configured to allow all traffic to flow in and out of the subnets with which it is associated. Each network ACL also includes a rule whose rule number is an asterisk (*). This rule ensures that if a packet doesn't match any

The network ACL also includes inbound rules that allow SSH and RDP traffic into the subnet. Outbound rule 120 enables responses to leave the subnet. The network ACL has outbound rules (100 and 110) that allow outbound HTTP and HTTPS traffic out of th



Everyone should be in a job they love.

Check out nextwork.org for more projects