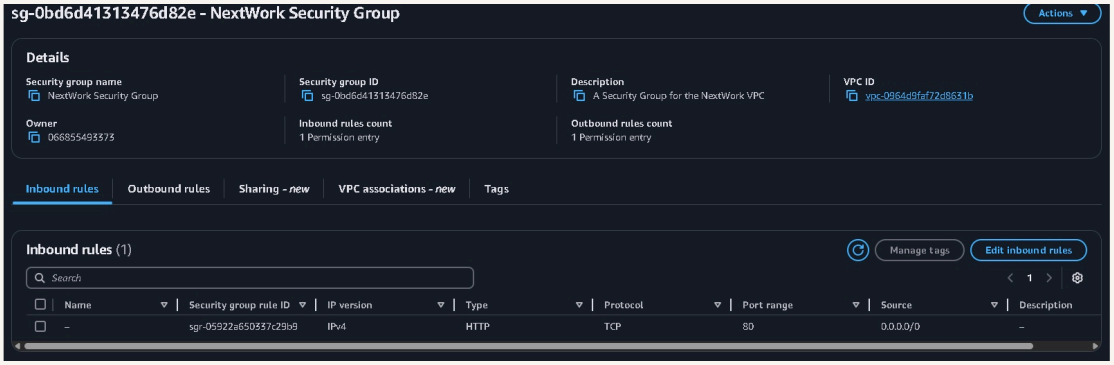
nextwork.org

VPC Traffic Flow and Security

Antonio C



Antonio C
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC lets you run AWS resources in a secure, isolated network—great for control, security, and scalability.

How I used Amazon VPC in this project

Route tables Internet gateways Network ACLs Security groups

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

One thing I didnt expect in this project is the configuration of inbound rules, outbound rules and subnet associations.

This project took me...

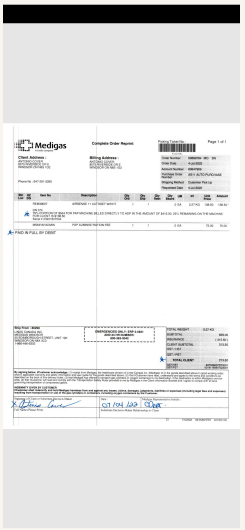
This project took me about an hour to complete.

Antonio C
NextWork Student

Route tables

Think of a route table as a GPS for the resources in your subnet. Just like a GPS helps people get to their destination in a city, a route table is a table of rules, called routes, that decide where the data in your network should go.

A route table is needed to make a subnet public because it directs traffic from the subnet to the internet via an Internet Gateway. Without this route, instances in the subnet can't send or receive traffic from the internet.

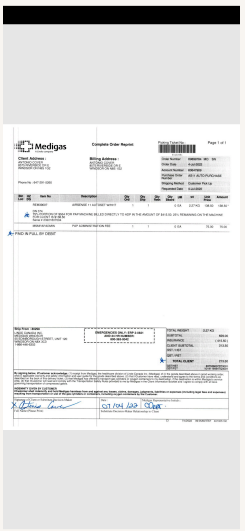


Antonio C
NextWork Student

Route destination and target

In a route, the destination defines the IP range of the traffic (e.g., 0.0.0.0/0 for all traffic), and the target specifies where to send that traffic (e.g., an Internet Gateway for public access or a NAT for private access).

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of 172.31.0.0/16 and a target of 0.0.0.0



A
Antonio C
NextWork Student

Security groups

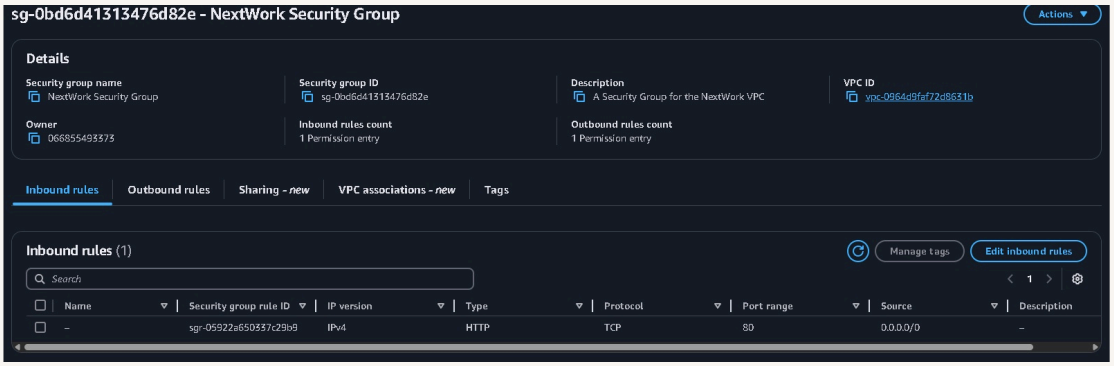
Security groups are responsible for checking who comes in and out. They have strict rules about what kind of traffic can enter or leave the resource based on its IP address, protocols and port numbers.

Inbound vs Outbound rules

Inbound rules control the data that can enter the resources in your security group, while outbound rules control which data that your resources can send out. I configured an inbound rule that has Type: HTTP Source: Anywhere-IPv4

By default, AWS security groups already allow all outbound traffic. Unless you specify otherwise, any resource associated with the security group can access and send data to any IP address - whether it's in any VPC VPCs and on the public internet

Antonio C
NextWork Student



A
Antonio C
NextWork Student

Network ACLs

Network ACLs are used to set broad traffic rules that apply to an entire subnet. For example, blocking incoming traffic from a particular range of IP addresses or denying all outbound traffic to certain ports.

Security groups vs. network ACLs

Network ACLs are used to set broad traffic rules that apply to an entire subnet. Security groups allow for more granular control, managing access to individual resource.

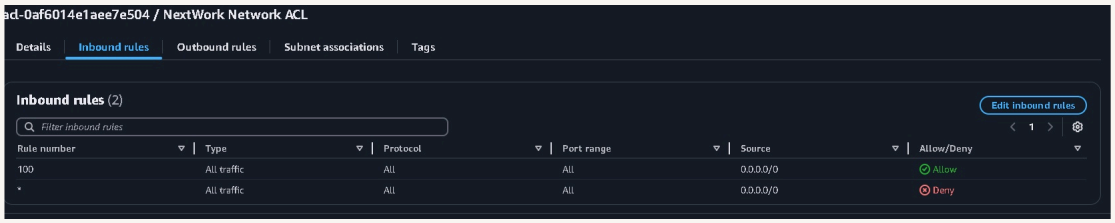
Antonio C
NextWork Student

Default vs Custom Network ACLs

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

The default network ACLs that AWS creates allow all inbound and outbound traffic.

For custom network ACLs that we create, all inbound and outbound traffic are denied until you add rules about the kind of traffic you'll allow.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects