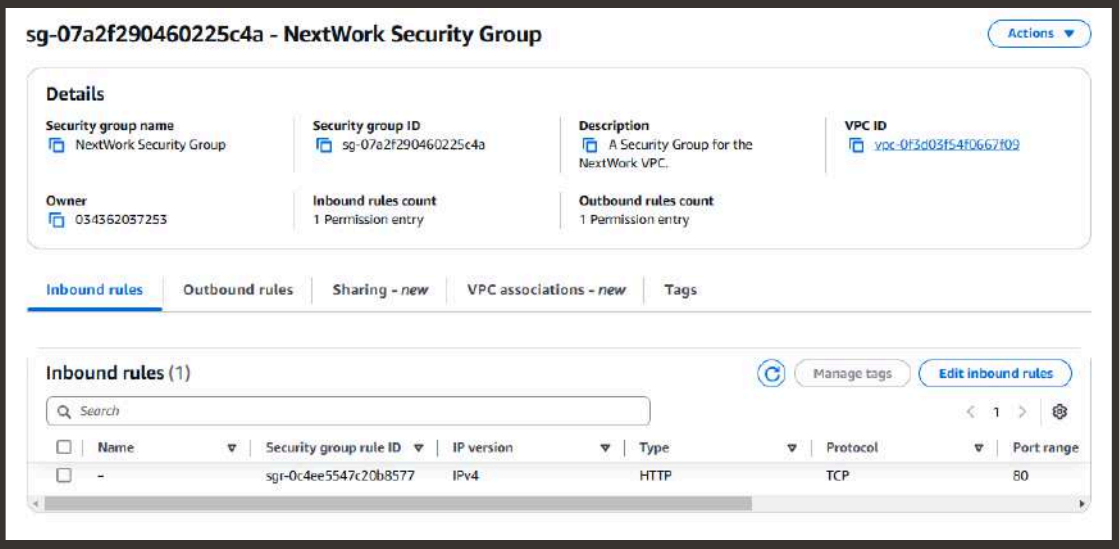
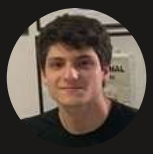
nextwork.org

VPC Traffic Flow and Security

Nicolás Aversa





Nicolás Aversa
NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that lets us launch AWS resources in a logically isolated virtual network that we define. It is useful because it gives us full control over our virtual networking environment.

How I used Amazon VPC in this project

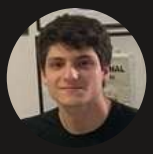
I used Amazon VPC in today's project to build on top of what I'd built in Series 1. In this project, I created a route table, a security group, and a network ACL.

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

One thing I did not expect in this project was to learn so much about network rules and protocols. I learned both hands-on and in theory in today's project.

This project took me...

This project took me an hour and a half, since I had to build the infrastructure of Series 1 all over again, to build on top of it.

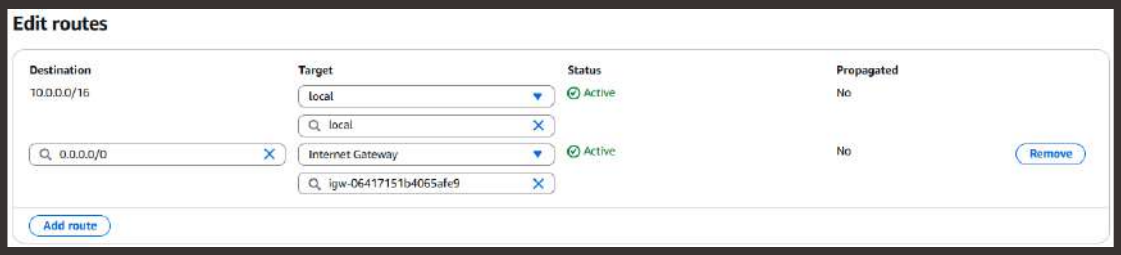


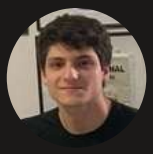
Nicolás Aversa
NextWork Student

Route tables

Route tables are a table of rules, called routes, that decide where the data in your network should go. This table tells the data where to travel (destination), and the path to travel (target) to get to its destination.

Routes tables are needed to make a subnet public because in order to let your subnet use an internet gateway, its route table must have a route that directs internet-bound traffic to the internet gateway. If not, it wouldn't know where to send data.



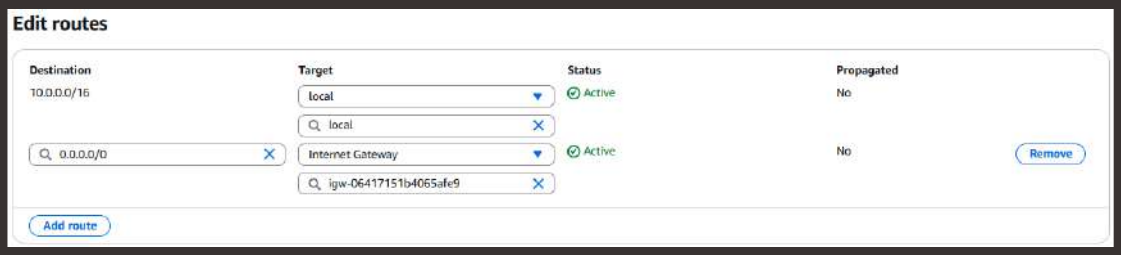


Nicolás Aversa
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the IP address range that traffic wants to reach, and the road that the traffic will have to take to get to 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' (any traffic that doesn't match 10.0.0.0/16) and a target of 'igw-06417151b4065afe9' (my Internet Gateway attached to my VPC).



Nicolás Aversa
NextWork Student

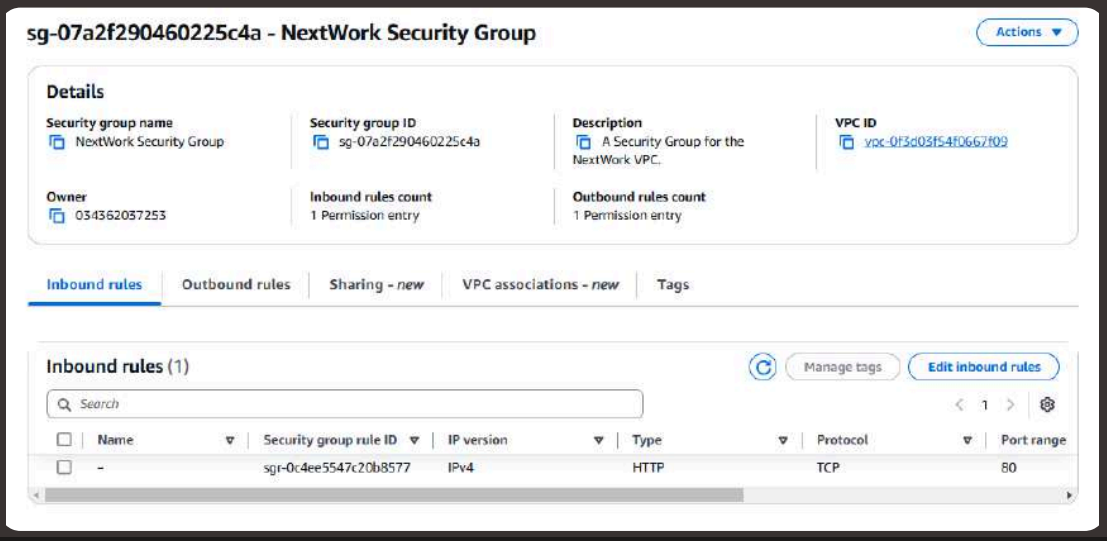
Security groups

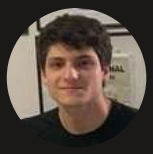
Security groups are like guards that protect our resources. They don't attach to a VPC or a subnet, they attach to a specific resource within that VPC or subnet; managing who comes in and out.

Inbound vs Outbound rules

Inbound rules are a security feature that lets us control the data that can enter/access the resources in the security group. I configured an inbound rule that allows anyone on the internet to access the public resources in my VPC/subnet.

Outbound rules are a security feature that lets us control the data that our resources can send out. By default, my security group's outbound rule was to allow all outbound traffic; meaning any resource can send data to any IP address.





Nicolás Aversa
NextWork Student

Network ACLs

Network ACLs are traffic guards that secure our subnet, checking each data packet (traffic) against a table of ACL rules before allowing them through. They limit what comes in and out of our public subnet.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that a security group is used to set rules to manage access to individual resources inside a subnet/VPC. On the other hand, a network ACL is used to set rules that affect the entire subnet.

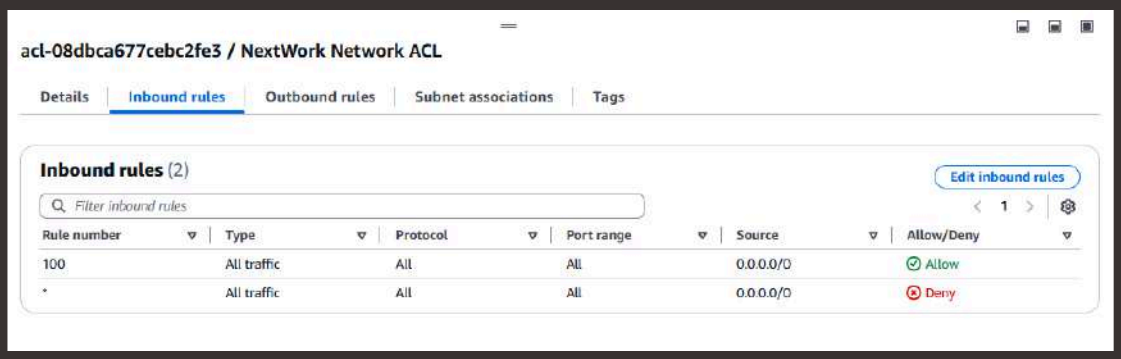
Nicolás Aversa
NextWork Student

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 to move freely. This is because 'Rule 100 Inbound' allows all inbound traffic into the Public Subnet and 'Rule 100 Outbound' allows all traffic out of the Public Subnet.

In contrast, a custom ACL's inbound and outbound rules are automatically set to 'Deny'. Meaning it denies all traffic into and out of the public subnet. This is why we have to add rules manually to specify what kind of traffic we'll allow.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects