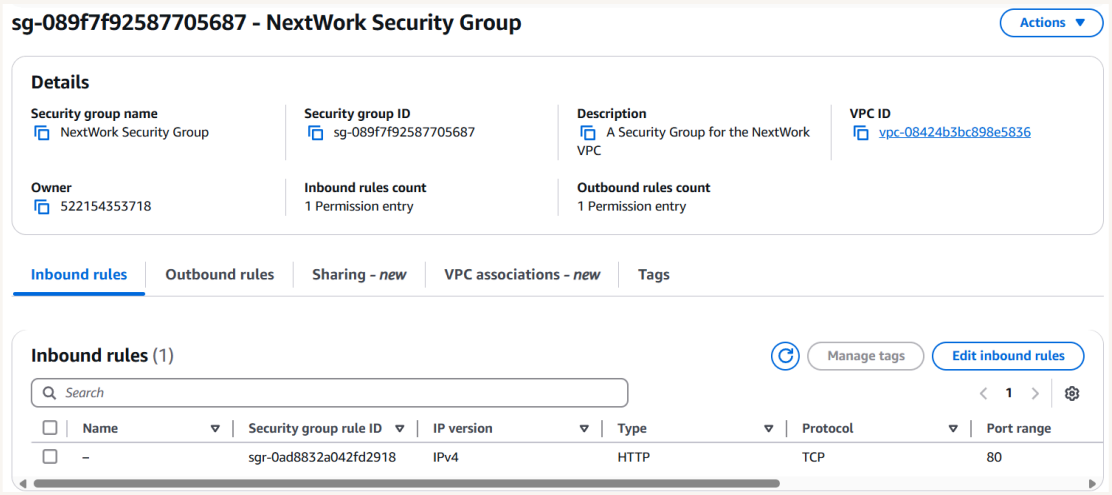
nextwork.org

VPC Traffic Flow and Security

LW lwazi995@outlook.com



LW
lwazi995@outlook.com
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

VPC are basically cities that have subnets, internet gateways for traffic that is outbound or inbound as well as different units to detect unauthorized traffic such as Security Groups and ACLs Network.

How I used Amazon VPC in this project

Amazon VPC provides a secure and scalable network, within AWS, enabling workload isolation,traffic control and hybrid connectivity. It enhances and scans unnecessary traffic by the rules set of the ACLs and Security groups.

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

I didn't expect the consepts to be explained in real life situations such as the use of cities, security gaurds and traffic cops it being VPC,Security groups and ACLs Networks.

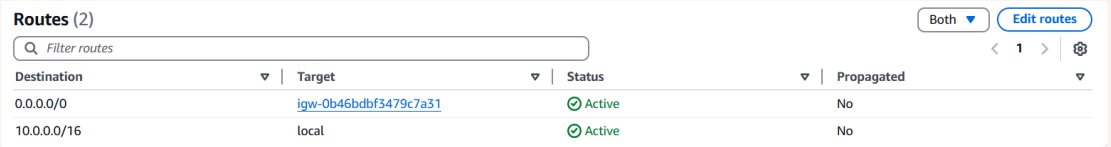
This project took me...

This project took me two hours and thirty min. Long but worth it.

Route tables

Route Tables are GPS that are within your VPC that have connection to the destination.

Route Tables are needed to make a subnet public because it has direct connectivity/route to the Internet Gateway in order for it to be considered public.

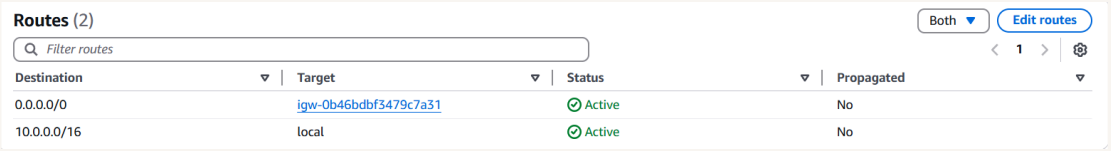


LW
lwazi995@outlook.com
NextWork Student

Route destination and target

Routes are defined by their destination and target which mean the destination is the range of IP addresses that traffic in my VPC is trying to reach. The target is the road or path that the traffic will use to get to the destination.

The route in my route table that directed internet-bound traffic to my internet gateway had a destination 0.0.0.0/0 and a target of the my NextWorkIG (Internet Gateway).



LW
lwazi995@outlook.com
NextWork Student

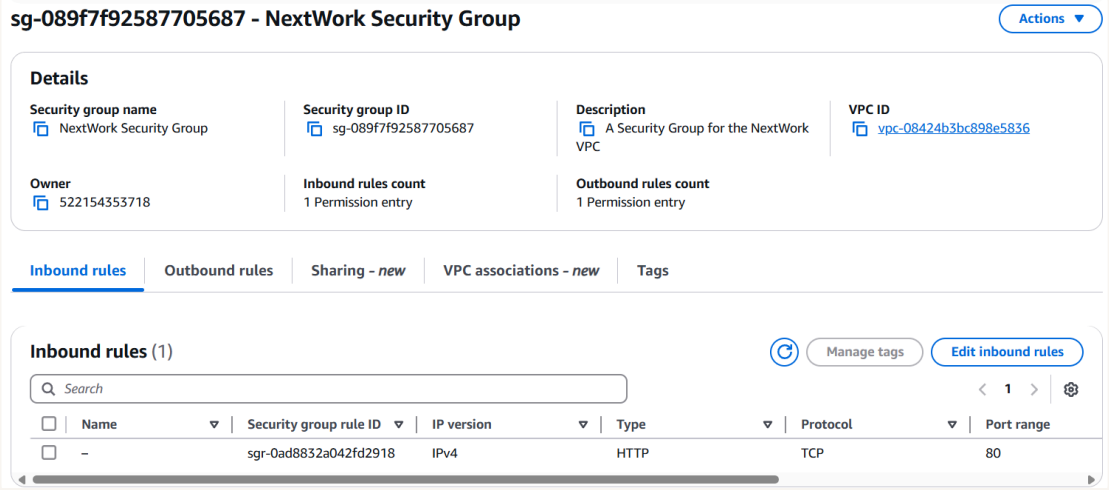
Security groups

Security Groups are security protocols/gaurd that detect traffic is allowed access towards the VPC or the resource level either its inbound or outbound. Every single resource in a VPC has a security group.

Inbound vs Outbound rules

Inbound rules are that monitor/restrict inbound traffic. I configured an inbound rule that restricts users visiting a web app im hosting.

Outbound rules are the rules that monitor/restrict outbound traffic. My security groups outbound rules my web app is requesting data from a public source. By default the outbound rule will allow all outbound traffic.



LW
lwazi995@outlook.com
NextWork Student

Network ACLs

Network ACLs are traffic officers verifying if the data packet/traffic/information is corresponding with the table of ACL rules before allowing them through. They stationed at every entry and exit point of our Subnet.

Security groups vs. network ACLs

The difference between security groups and a network ACL is that, ACL are set to check data packets and review them if they correspond with the ACL rules set to allow or deny access. Security groups secure resources at a resources level.

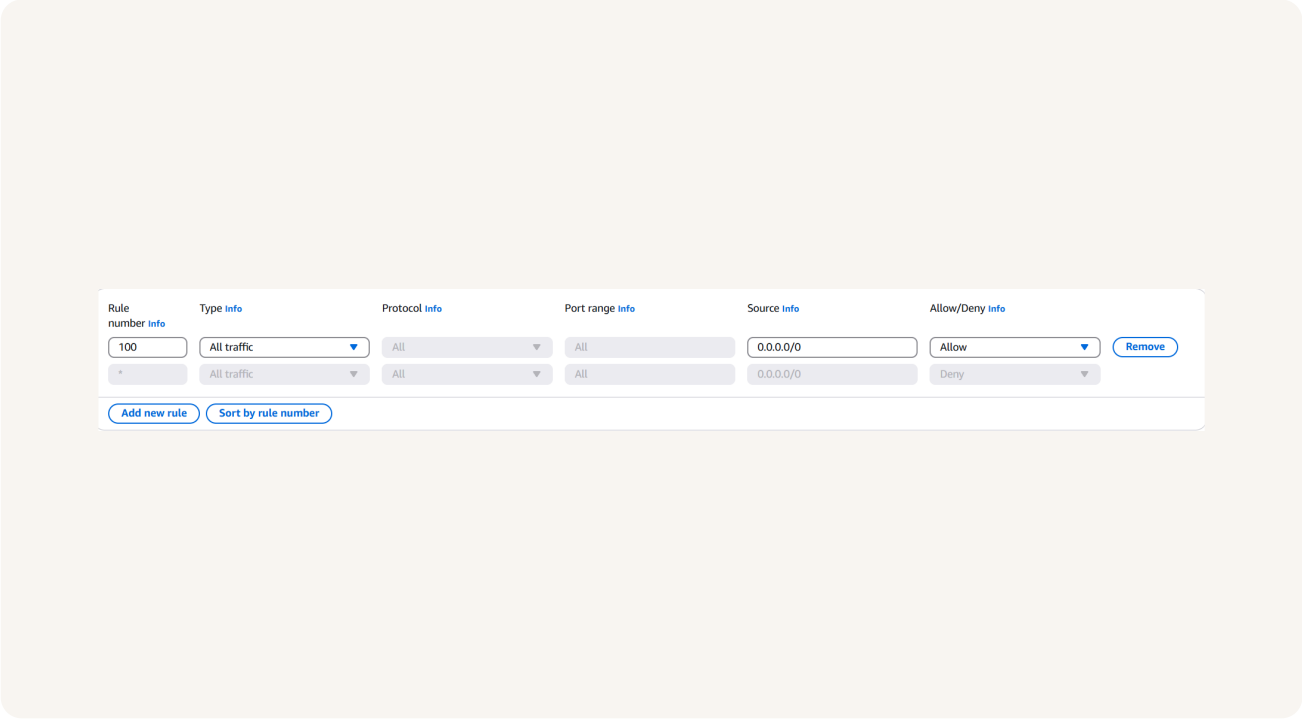
LW
lwazi995@outlook.com
NextWork Student

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 rules will be standard to start with 100 low numbers go first

In contrast, a custom ACL''s inbound and outbound rules are automatically set to deny all incoming outgoing traffic



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects