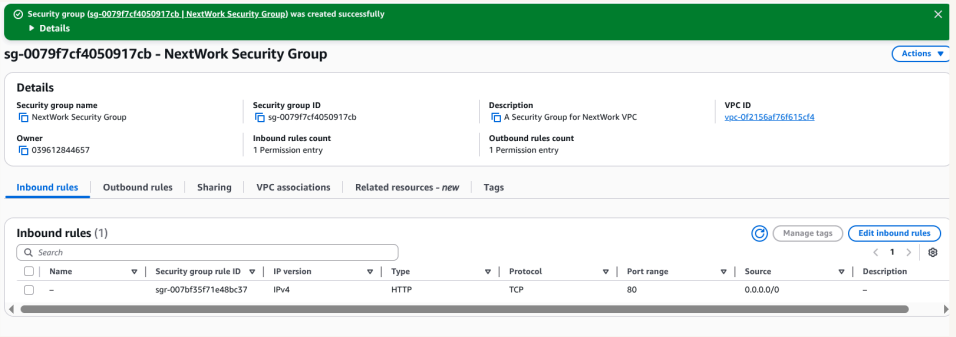
nextwork.org

VPC Traffic Flow and Security

Katleo Rantle



Katleo Rantle
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is logical network boundary in the cloud and it is useful because it provides security and privacy to our resources on the cloud

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to setup multiple layers of security NACL at subnet level and security groups at resource level.

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

One thing I didn't expect in this project was bing able to view all my VPC resources across multiple regions from a single screen

This project took me...

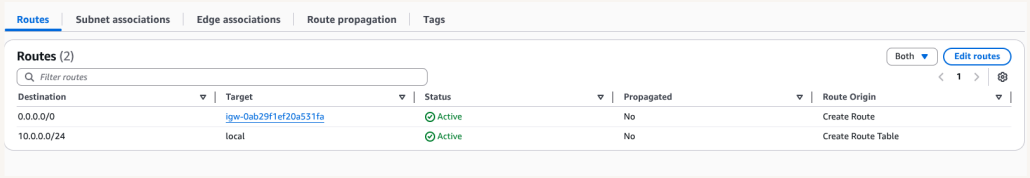
This project took me 2.5hrs

Katleo Rantle
NextWork Student

Route tables

Route tables are rules that detemine where data in our network should go

Routes tables are needed to make a subnet public because internet bound traffic needs a route that directs that traffic to the IGW without it that traffic will not be allowed to leave the VPC thus it cannot be public

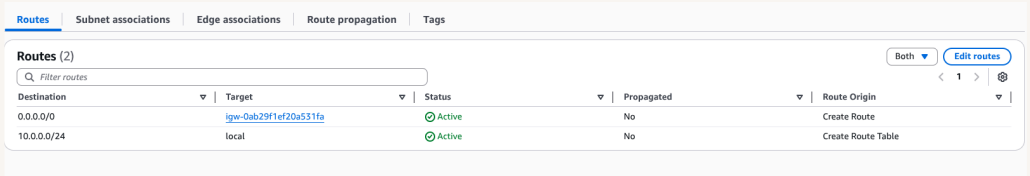


Katleo Rantle
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean where the taffic wants to go, ip address range (destination) and how the traffic will get there, the path (target)

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 igw-0ab29f1ef20a531fa



Katleo Rantle
NextWork Student

Security groups

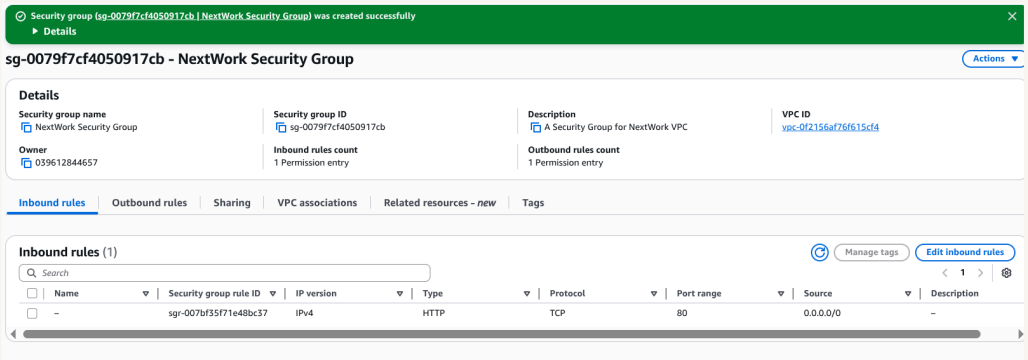
Security groups are rules that can control what kind of data or traffic is allowed to enter or leave a resource

Inbound vs Outbound rules

Inbound rules are rules that contol what kind of traffic can enter the resource in the security group I configured an inbound rule that allows any external device to communicte with our resource

Outbound rules are rules that define or contol data that our resouce can send By default, my security group's outbound rule allow any resource within our secuirty group to send data to any ip address

Katleo Rantle
NextWork Student



Katleo Rantle
NextWork Student

Network ACLs

Network ACLs are rules that control traffic or check data packets at subnet level to see what may or may not enter

Security groups vs. network ACLs

The difference between a security group and a network ACL is that NACLs work at a subnet level and can block entire classes of ip addresses and security groups work at resource level

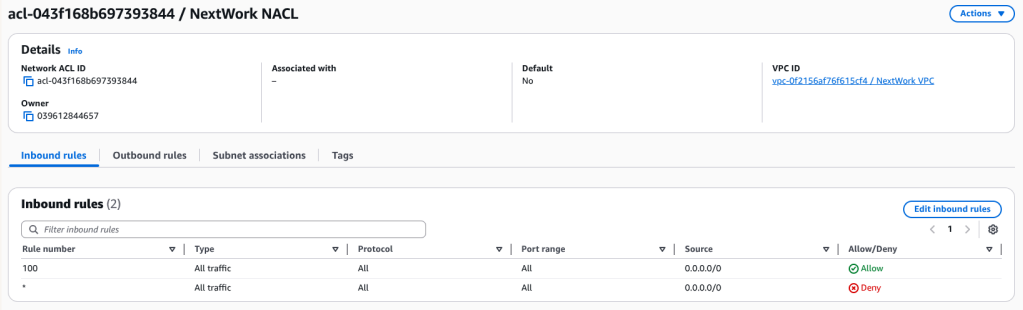
Katleo Rantle
NextWork Student

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 inbound and out bound traffic

In contrast, a custom ACL’s inbound and outbound rules are automatically set to denie all traffic untill we add the rules for what kind of traffic we allow



Katleo Rantle
NextWork Student

Tracking VPC Resources

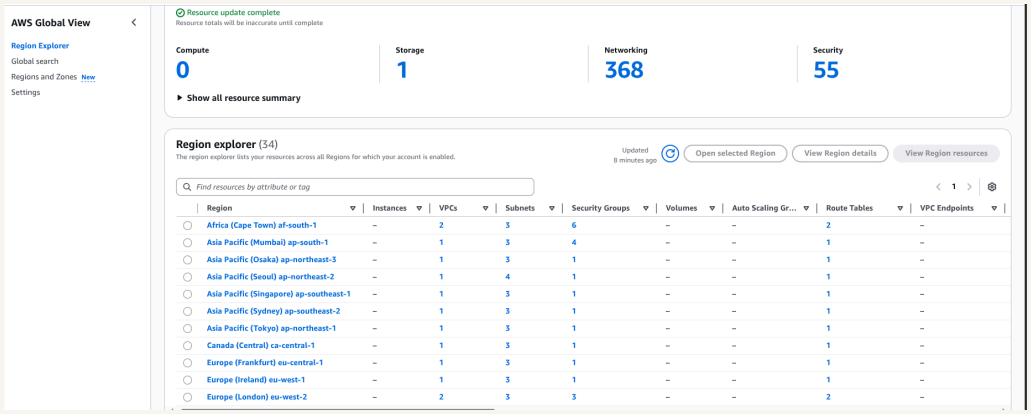
I created additional VPC, internet gateway and security group Instead of my usual region, I used eu-west-2, london Teams would use multiple regions to improve latency and make apps more highly available ie protect from natural diasters and other things that can go wrong from working only in one geograpical location

EC2 Global View is a tool where you can find and manage all ec2 and VPC resources accross all regions I could even narrow down my search by specific region Without EC2 Global View, you'd have to go into the specific region to be able to see resources in that region

Now that I've learnt about EC2 Global View, I'd use it again in cases where Ec2 and VPC resources have been delpoyed accross multiple regions

Katleo Rantle
NextWork Student

nextwork.org



The place to learn & showcase your skills

Check out nextwork.org for more projects