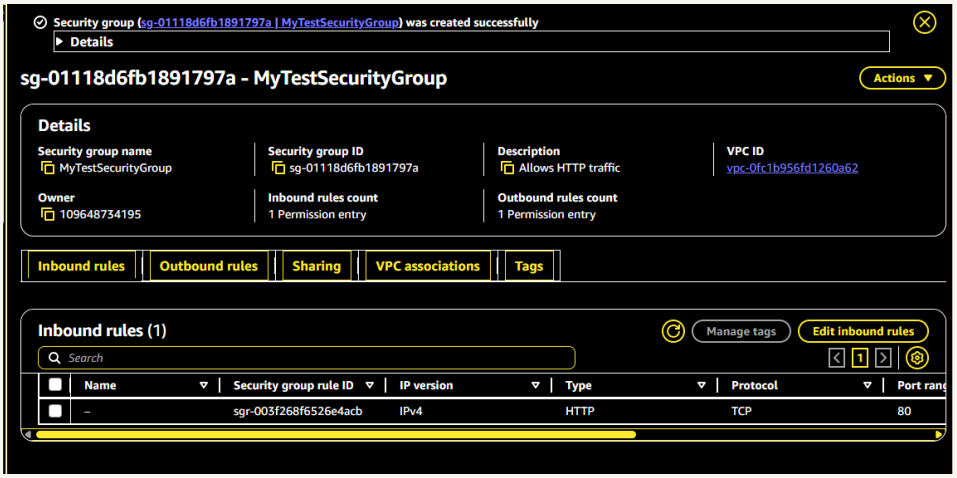
nextwork.org

VPC Traffic Flow and Security

Michael K.



Michael K.
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a logically isolated virtual network within AWS where i can launch and manage AWS resources (such as EC2 instances, RDS databases, and load balancers) using my own defined IP address range, subnets, route tables, and network gateways.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create my own virtual private network, and configure a secure traffic within it.

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

One thing I didn't expect in this project was the complexity to understand why and how to set up the subnet with the Route Table and Network ACL.

This project took me...

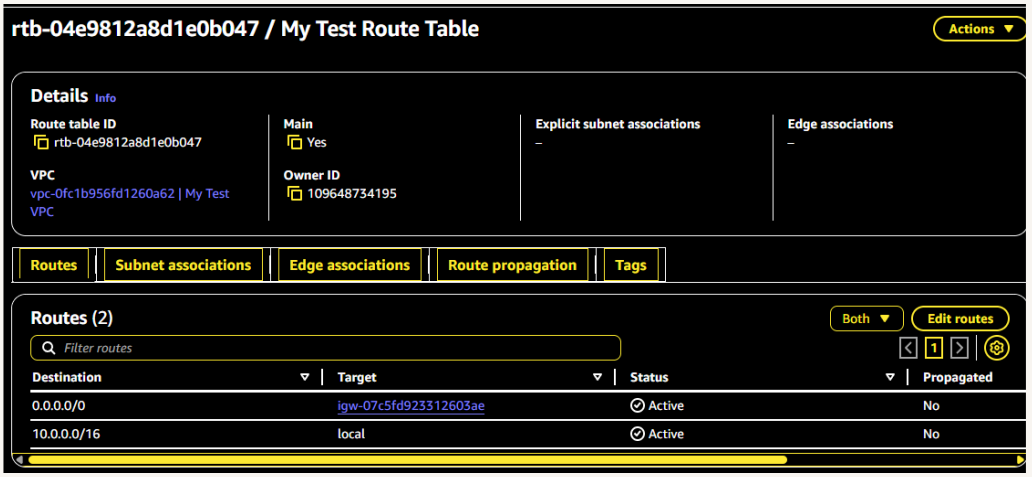
This project took me 2 hours

Michael K.
NextWork Student

Route tables

Route tables are like GPS which guides the traffic within our VPC to it destination.

Routes tables are needed to make a subnet public because for a subnet to be made public it has to be attached to a route which will lead its traffic to the Internet gateway. The subnet will be attached to that route through an explicit association to the route tables. As that traffic reaches the Internet gateway it will be sent to the Internet. As soon as the traffic from that subnet reaches the IGW, it is made public since it is sent to the Internet directly after.

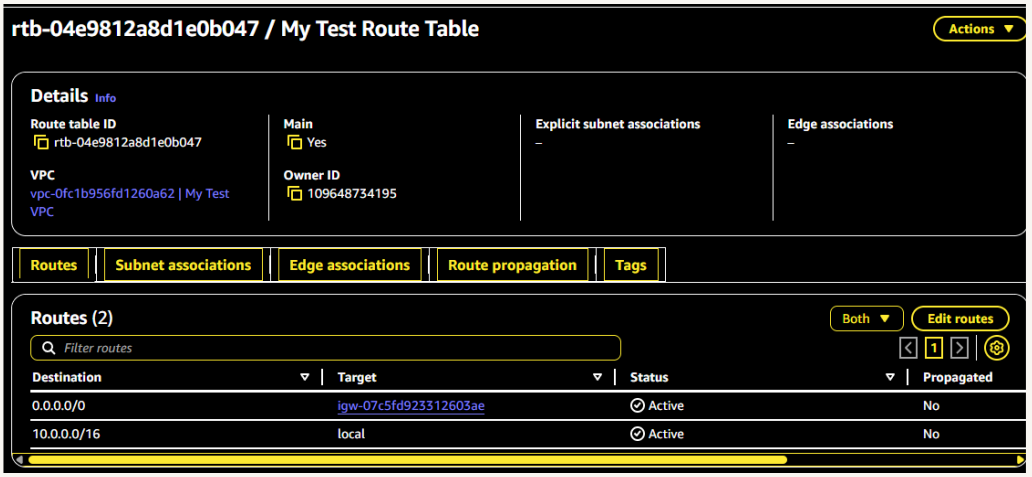


Michael K.
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the place where the traffic needs to be sent and the route that the traffic needs to take to reach that 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 which means any destination (any ip-adress) and a target of the already created IGW, since it is considered that the destination not being a resource in the VPC is automatically somewhere in the Internet.



J
Michael K.
NextWork Student

Security groups

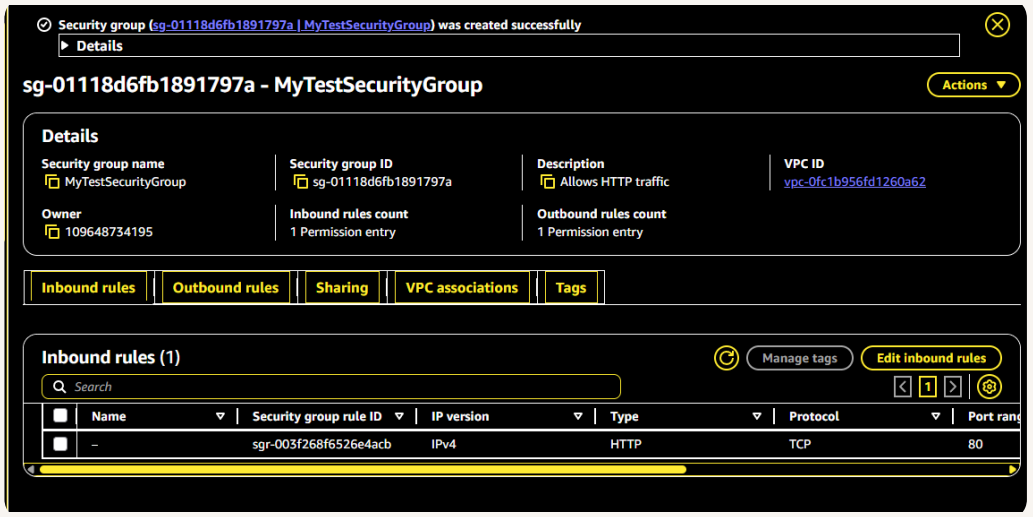
Security groups are statements (security checkpoint) which control traffic in (inbound traffic) and out (outbound traffic) of EC2 Instances.

Inbound vs Outbound rules

Inbound rules are statements that define the kind of traffic that can enter a resource. I configured an inbound rule that ONLY HTTP traffics with an IPv4 address from anywhere can enter my resource.

Outbound rules are statements that define the kind of traffic that can leave a resource. By default, my security group's outbound rule is letting everything from the resource out.

Michael K.
NextWork Student



Michael K.
NextWork Student

Network ACLs

Network ACLs are security gurds at the entry and exit of subnets, controlling data packets (traffic) with the use of ACLs rules before letting them in or out.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups works at the resource level while NACL works and the subnet level. NACL is stateless while Security groups are stateful.

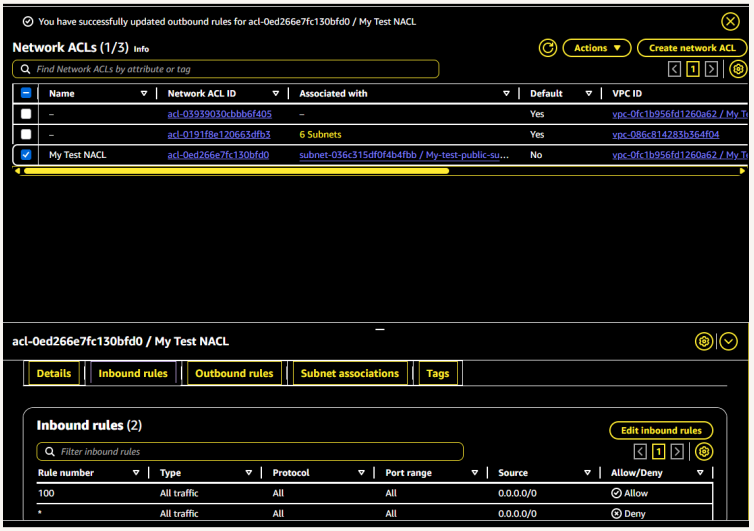
Michael K.
NextWork Student

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 entrying or leaving the subnet.

In contrast, a custom ACL’s inbound and outbound rules are automatically set to allow or deny the entry or exit of data packet (traffic) whose features (protocols, IP Adresses etc.) are or are not part of the customized or defined rule.



J

Michael K.
NextWork Student

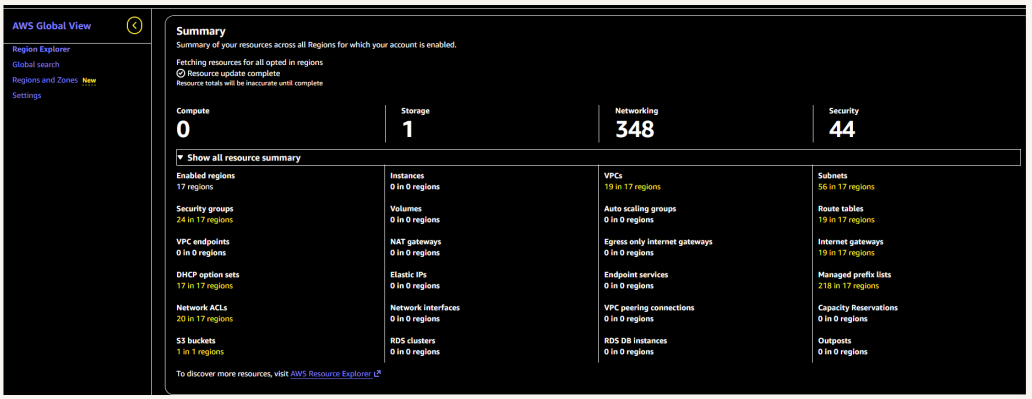
Tracking VPC Resources

I created additional resources (VPC, Internet Gateway and Security Groups) through the CLI. Instead of my usual region, I used another region. Teams would use multiple regions to reduce latency and enable fault tolerance.

EC2 Global View is a tool where you can find all the resources created in my account. I could even narrow down my search by searching for resources in a particular region. Without EC2 Global View, you'd have to everything said up manually.

Now that I've learnt about EC2 Global View, I'd use it again to have an Insight to the resources created in my account.

Michael K.
NextWork Student



The place to learn & showcase your skills

Check out nextwork.org for more projects